User Guide

SURFboard® eXtreme

SBG6782-AC Wireless Cable Modem & Router with MoCA® Networking

© 2013 ARRIS Enterprises, Inc. All rights reserved.

No part of this publication may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from ARRIS Enterprises, Inc. (“ARRIS”). ARRIS reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of ARRIS to provide notification of such revision or change.

ARRIS and the ARRIS logo are trademarks or registered trademarks of ARRIS Enterprises, Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and the names of their products. ARRIS disclaims proprietary interest in the marks and names of others.

MOTOROLA, SURFboard, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC, and are used by ARRIS under license. All other product or service names are the property of their respective owners.

ARRIS provides this guide without warranty of any kind, implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. ARRIS may make improvements or changes in the product(s) described in this manual at any time.

Safety and Regulatory Information

IMPORTANT SAFETY INSTRUCTIONS

- **Read This Before You Begin** — When using your equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons, including the following:
- Read all of the instructions listed here and/or in the user manual before you operate this device. Give particular attention to all safety precautions. Retain the instructions for future reference.
- This device must be installed and used in strict accordance with manufacturer's instructions, as described in the user documentation that is included with the device.
- Comply with all warning and caution statements in the instructions. Observe all warning and caution symbols that are affixed to this device.
- To prevent fire or shock hazard, do not expose this device to rain or moisture. The device must not be exposed to dripping or splashing. Do not place objects filled with liquids, such as vases, on the device.
- This device was qualified under test conditions that included the use of the supplied cables between system components. To ensure regulatory and safety compliance, use only the provided power and interface cables and install them properly.
- Different types of cord sets may be used for connections to the main POWER supply circuit. Use only a main line cord that complies with all applicable device safety requirements of the country of use.
- Installation of this device must be in accordance with national wiring codes and conform to local regulations.
- Operate this device only from the type of power source indicated on the device's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Do not overload outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded electrical outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard.
- Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit from the device.
- Place this device in a location that is close enough to an electrical outlet to accommodate the length of the power cord.
- Place the device to allow for easy access when disconnecting the power cord of the device from the electrical wall outlet.
- Do not connect the plug into an extension cord, receptacle, or other outlet unless the plug can be fully inserted with no part of the blades exposed.
- Place this device on a stable surface.
- Avoid damaging the device with static by touching the coaxial cable when it is attached to the earth-grounded coaxial cable-TV wall outlet.
- Always first touch the coaxial cable connector on the device when disconnecting or reconnecting the Ethernet cable from the device or user's PC.

- It is recommended that the customer install an electrical surge protector in the electrical outlet to which this device is connected. This is to avoid damaging the device by local lightning strikes and other electrical surges.
- Postpone installation until there is no risk of thunderstorm or lightning activity in the area.
- Do not use this product near water: for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement, or near a swimming pool.
- Do not cover the device or block the airflow to the device with any other objects. Keep the device away from excessive heat and humidity and keep the device free from vibration and dust.
- Wipe the device with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the device or use forced air to remove dust.
- For added protection, unplug the device from the wall outlet and disconnect the cables to avoid damage to this device during lightning activity or power surges.
- Upon completion of any service or repairs to this device, ask the service technician to perform safety checks to determine that the device is in safe operating condition.
- Do not open the device. Do not perform any servicing other than that contained in the installation and troubleshooting instructions. Refer all servicing to qualified service personnel.

This device should not be used in an environment that exceeds 104º F (40º C).

SAVE THE ABOVE INSTRUCTIONS

Note to CATV System Installer — This reminder is provided to call the CATV system installer's attention to Article 820.93 and 820.100 of the National Electric Code, which provides guidelines for proper grounding and, in particular, specifies that the Coaxial cable shield shall be connected to the grounding system of the building, as close to the point of cable entry as practical.

FCC STATEMENTS

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the device and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

FCC CAUTION: Any changes or modifications not expressly approved by Motorola for compliance could void the user's authority to operate the equipment.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To comply with the FCC RF exposure compliance requirements, the separation distance between the antenna and any person's body (including hands, wrists, feet and ankles) must be at least 20 cm (8 inches).

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter except those already approved in this filing.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destinations. The firmware setting is not accessible by the end user.

INDUSTRY CANADA (IC) STATEMENT

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

- This device may not cause interference, and
- This device must accept any interference, including interference that may cause undesired operation of the device.

CAN ICES-3 (B)/NMB-3 (B)

In Canada, RLAN devices are restricted from using the 5600-5650 MHz frequency band.

CAUTION: To reduce the potential for harmful interference to co-channel mobile satellite systems, use of the 5150-5250 MHz frequency band is restricted to indoor use only.

High power radars are allocated as primary users (meaning they have priority) of 5250-5350 MHz and 5650-5850 MHz frequency bands. These radars could cause interference and/or damage to License Exempt–Local Area Network (LE-LAN) devices.

IC RADIATION EXPOSURE STATEMENT

IMPORTANT NOTE: This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

AVIS D'INDUSTRIE CANADA (IC)

Cet appareil est conforme à la réglementation RSS-210 d'Industrie Canada. Son utilisation est assujettie aux deux conditions suivantes :

- Cet appareil ne doit pas causer d'interférences et
- Cet appareil doit accepter toute interférence reçue, y compris les interférences causant un fonctionnement non désiré.

CAN ICES-3 (B)/NMB-3 (B)

Au Canada, les appareils de réseau local sans fil ne sont pas autorisés à utiliser les bandes de fréquence 5600-5650 MHz.

AVERTISSEMENT: afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux, les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur

Les radars à haute puissance sont définis en tant qu'utilisateurs principaux (c.-à-d. prioritaires) des bandes de fréquences 5250-5350 MHz et 5650-5850 MHz. Ces radars peuvent causer de l'interférence ou des dommages susceptibles de nuire aux appareils exempts de licence–réseau local (LAN-EL).

DÉCLARATION DE IC SUR L'EXPOSITION AUX RAYONNEMENTS

NOTE IMPORTANTE: cet équipement est conforme aux limites d'exposition aux rayonnements établies par IC pour un environnement non contrôlé. Cet équipement doit être installé et utilisé de manière à maintenir une distance d'au moins 20 cm entre la source de rayonnement et votre corps.

WIRELESS LAN INFORMATION

This device is a wireless network product that uses Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency-Division Multiple Access (OFDMA) radio technologies. The device is designed to be interoperable with any other wireless DSSS and OFDMA products that comply with:

- The IEEE 802.11 Standard on Wireless LANs (Revision AC, Revision B, Revision G, and Revision N), as defined and approved by the Institute of Electrical Electronics Engineers
- The Wireless Fidelity (Wi-Fi) certification as defined by the Wireless Ethernet Compatibility Alliance (WECA).

Restrictions on the Use of Wireless Devices

In some situations or environments, the use of wireless devices may be restricted by the proprietor of the building or responsible representatives of the organization. For example, using wireless equipment in any environment where the risk of interference to other devices or services is perceived or identified as harmful.

If you are uncertain of the applicable policy for the use of wireless equipment in a specific organization or environment, you are encouraged to ask for authorization to use the device prior to turning on the equipment.

The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this product, or the substitution or attachment of connecting cables and equipment other than specified by the manufacturer. Correction of the interference caused by such unauthorized modification, substitution, or attachment is the responsibility of the user.

The manufacturer and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from failing to comply with these guidelines.

Note: The use of the 5150-5250 MHz frequency band is restricted to Indoor Use Only.

SECURITY WARNING: This device allows you to create a wireless network. Wireless network connections may be accessible by unauthorized users. For more information on how to protect your network, see Change the Default Username and Password in this guide for instructions or visit the ARRIS website.

CARING FOR THE ENVIRONMENT BY RECYCLING

When you see this symbol on an ARRIS product, do not dispose of the product with residential or commercial waste.

Recycling your ARRIS Equipment

Please do not dispose of this product with your residential or commercial waste. Some countries or regions, such as the European Union, have set up systems to collect and recycle electrical and electronic waste items. Contact your local authorities for information about practices established for your region. If collection systems are not available, call ARRIS Customer Service at **1-877-466-8646** for assistance.

Contents

Safety and Regulatory Information ..... **i**
Getting Started **1**
Introduction 1
In the Box 1
Additional Items You May Need 2
System Requirements 2
Contact Information 2
Product Overview **3**
Front Panel 3
Wi-Fi Protected Setup (WPS) 4
Rear Panel 5
Gateway Label 5
Installing Your Gateway **6**
Connect the Gateway to Your Computer 6
Test the Gateway Connections 7
Connect Your MoCA-Enabled Devices 7
Setting Up an Internet Connection **8**
Configure Your IP Address 8
Verify & Renew Your IP Address 11
Setting Up a Wireless Network Connection **12**
Launch the Quick Start Wizard to Set Up Your Wireless Network 12
Manually Set Up a Wireless Network on Your Computer 13
Connect Your WPS-Enabled Devices 14
Test Your Wireless Network Connection 14
Managing Your Gateway and Connected Networks **15**
Start the Gateway Web Manager 15
Gateway Web Manager Menu Options 16
Get Help 17
View the Gateway Product Information 19
View the Gateway Status 19
Back Up Your Gateway Settings 20
Restore Your Gateway Settings 21
Reset to Factory Defaults 21
Exit the SBG6782-AC Web Manager 22
Configuring Your MoCA Network **23**
Set Up Your MoCA Network 23

Protecting & Monitoring Your Wireless Network 24
Prevent Unauthorized Access 24
Change the Default User Name and Password 24
Set Up Firewall Protection 26
Set Up Parental Controls 27
Set Up Port Triggers 28
Set Up the DMZ Host 29
Store Remote Firewall Logs 30
Troubleshooting Tips 31
Solutions 31
Front Panel LED Icons and Error Conditions 32
Gateway Configuration Screen Definitions 33
Basic Screens 33
Setup 33
DHCP 35
DDNS 36
Backup and Restore 37
MoCA 37
Firewall Screens 38
Protection Level 38
Parental Control 40
Local Log 41
Remote Log 42
Warranty Information 44

Tables

Table 1 – SBG6782-AC Package Contents 1
Table 2 – SBG6782-AC Front Panel LED Icons 3
Table 3 – SBG6782-AC Rear Panel Ports & Connectors 5
Table 4 – SBG6782-AC Web Manager Main Menu Options 16
Table 5 – Troubleshooting Solutions 31
Table 6 – Front Panel LED Icons and Error Conditions 32
Table 7 – Basic Setup Screen-Field Descriptions 34
Table 8 – Basic DHCP Screen-Field Descriptions 35
Table 9 – Basic DDNS Screen-Field Descriptions 36
Table 10 – Basic Backup & Restore-Field Descriptions 37
Table 11 – Basic MoCA Screen-Field Descriptions 38
Table 12 – Firewall Protection Level Screen-Field Descriptions 39

Table 13 – Firewall Parental Control-Field Descriptions 40
Table 14 – Firewall Local Log Screen-Field Descriptions 42
Table 15 – Firewall Remote Log Screen-Field Descriptions 43

Figures

Figure 1 – SBG6782-AC Front View 3
Figure 2 – SBG6782-AC Rear View 5
Figure 3 – SBG6782-AC Connection Diagram 6
Figure 4 – SBG6782-AC Quick Start Wizard Screen 13
Figure 5 – Quick Start Wizard Opening Screen 15
Figure 6 – SBG6782-AC Web Manager Main Menu Buttons 16
Figure 7 – SBG6782-AC Web Manager Main Menu Links 16
Figure 8 – Help Overview Screen 17
Figure 9 – Help About Screen 18
Figure 10 – SBG6782-AC Status – Product Information Screen 19
Figure 11 – SBG6782-AC Status Connection Screen 20
Figure 12 – SBG6782-AC Backup and Restore Screen 20
Figure 13 – Restore Factory Defaults 22
Figure 14 – MoCA Configuration and Status Screen 23
Figure 15 – Change Username 25
Figure 16 – Change User Password 26
Figure 17 – Firewall Protection Level Screen 26
Figure 18 – Parental Control-Change Time Zone Screen 27
Figure 19 – Firewall Parental Control Screen 28
Figure 20 – Advanced Port Triggers Screen 29
Figure 21 – Advanced DMZ Host Screen 29
Figure 22 – Firewall Remote Log Screen 30
Figure 23 – Basic Setup Screen 33
Figure 24 – Basic DHCP Screen 35
Figure 25 – Basic DDNS Screen 36
Figure 26 – Basic Backup & Restore Screen 37
Figure 27 – Basic MoCA Configuration and Status Screen 37
Figure 28 – Firewall Protection Level Screen 39
Figure 29 – Firewall Parental Control Screen 40
Figure 30 – Firewall Local Log Screen 41
Figure 31 – Firewall Remote Log Screen 43

1 Getting Started

Introduction

Welcome to the next generation of ultra high-speed Wi-Fi gateways. Your new Motorola SURFboard® eXtreme SBG6782-AC Wireless Cable Modem & Router with MoCA® (Multimedia over Coax) provides a home network with wireless high-speed data and multimedia service access. With built-in MoCA technology, the SBG6782-AC also provides high-speed Internet access to multiple MoCA-enabled devices using the existing coaxial cable connection in your home. You can also expand your MoCA home network using the Motorola SBM1000 Video Adapter Kit, sold separately. The SBG6782-AC includes a Wi-Fi Pairing option for quick and easy connections for your wireless devices.

This guide provides instructions for installing and configuring the SBG6782-AC gateway, setting up a secure wireless network connection, and managing your gateway and network configurations.

In the Box

Before installing your new wireless cable modem gateway, check that the following items are included in the box. If any items are missing, please call ARRIS SURFboard Technical Support at **1-877-466-8646**.

Table 1 – SBG6782-AC Package Contents

ITEM		DESCRIPTION
SBG6782-AC Wireless Gateway		Wireless high-speed cable modem and router with MoCA
Power Cord		Provides power to the gateway through an electrical outlet connection
Ethernet Cable		Standard Cat 5 or higher cable for connecting to the network
Software License & Regulatory Card		Contains software license, warranty, and safety information for the gateway

ITEM		DESCRIPTION
SBG6782-AC Quick Start Guide		Provides basic information for connecting the gateway

Additional Items You May Need

- Coaxial cable, if one is not already connected to a cable wall outlet
- Ethernet cable for each additional Ethernet-enabled device
- RF splitter (for additional coaxial cable connections, e.g., set-top box, Smart TV)

System Requirements

- High-speed Internet access account
- Web browser access, such as Microsoft Internet Explorer, Firefox, Google Chrome, or Safari
- Compatible operating systems:
  - Windows® 8
  - Windows 7 Service Pack 1 (SP1)
  - Windows Vista™ SP2
  - Windows XP SP3
  - Mac® 10.4 or higher
  - UNIX®
  - Linux®

Contact Information

For technical support and additional ARRIS/Motorola product information, please visit the ARRIS Support website at www.arrisi.com/consumer.

You can also call ARRIS SURFboard Technical Support at **1-877-466-8646**. When you call, you will need the following information from the product label located on the bottom of the SBG6782-AC:

- Gateway model number (**SBG6782-AC**)
- Gateway serial number (**S/N**)

2 Product Overview

Front Panel

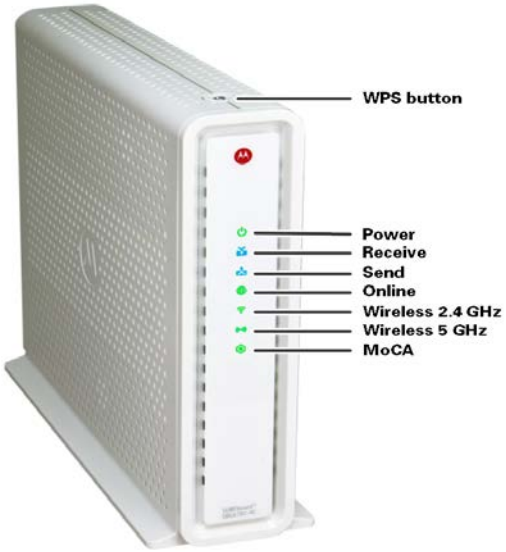


Figure 1 – SBG6782-AC Front View

Table 2 – SBG6782-AC Front Panel LED Icons

BUTTON/LED ICON	FLASHING	ON
WPS Button	Not applicable — no LED on button.	Not applicable — no LED on button. See Wi-Fi Protected Setup (WPS) for more information.
POWER	Not applicable — icon does not flash.	**Green**: Power is properly connected.
RECEIVE	Scanning for a downstream (receive) channel connection	**Green**: Non-bonded downstream channel is connected. **Blue***: High-speed Internet connection with bonded downstream channels.

BUTTON/LED ICON	FLASHING	ON
SEND	Scanning for an upstream (send) channel connection	**Green**: Non-bonded upstream channel is connected **Blue***: High-speed Internet connection with bonded upstream channels
ONLINE	Scanning for an Internet connection	**Green**: Gateway is connected to the network
WIRELESS	**Green**: Wi-Fi enabled with encrypted wireless data activity. **Amber**: Wi-Fi enabled with unencrypted wireless data activity	**Green**: 2.4 GHz wireless connection is made between the SBG6782-AC and another Wi-Fi enabled device on your network; for example, printer, tablet, or laptop. **Amber**: Flashes during the wireless pairing process and lights SOLID **green** after five seconds or less.
WIRELESS	**Green**: Wi-Fi enabled with encrypted wireless data activity. **Amber**: Wi-Fi enabled with unencrypted wireless data activity	**Green**: 5 GHz wireless connection is made between the SBG6782-AC and another Wi-Fi enabled device on your network; for example, printer, tablet, or laptop. **Amber**: Flashes during the wireless pairing process and lights SOLID **green** after five seconds or less.
MoCA	**Green**: Indicates MoCA activity in progress	**Green**: A MoCA-enabled device is connected and running.

***Blue** - Indicates DOCSIS 3.0 operation (high-speed Internet access) which may not be available in all locations. Check with your service provider for availability in your area.

Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is a wireless network setup option that provides a quick and easy solution for setting up a secure wireless network connection for any WPS-enabled device; such as a computer or printer. WPS automatically configures your wireless network connections and sets up wireless security. See Connect Your WPS-Enabled Devices for more information.

Rear Panel

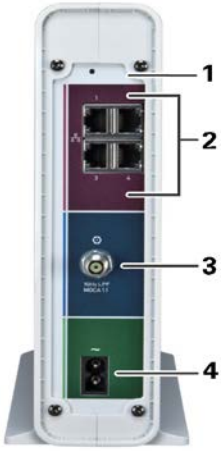


Figure 2 – SBG6782-AC Rear View

Table 3 – SBG6782-AC Rear Panel Ports & Connectors

	PORT NAME	DESCRIPTION
1	**RESET button**	Recessed button to reset the gateway factory settings When RESET is pushed and held for five seconds, the default factory settings are restored and the gateway is rebooted **WARNING!** RESET also deletes all of your custom gateway configurations.
2	1 2 3 4 ETHERNET	Four one-gigabit Ethernet ports for RJ-45 cable connections **Green** LED is ON - Indicates a data transfer rate of one gigabit per second **Amber** LED is ON - Indicates a data transfer rate of less than one gigabit per second
3	CABLE	Coaxial Cable connector
4	POWER	100 - 240VAC Power connector

Gateway Label

The SBG6782-AC gateway product label is located on the bottom of the gateway. It contains specific gateway ID information that you may need when contacting your service provider or the ARRIS SURFboard Technical Support Center.

To receive Internet access, please contact your service provider for assistance. Make sure you have the Gateway model number (**SBG6782-AC**) and Serial number (**S/N**) located on the gateway label.

3 Installing Your Gateway

This product is for indoor use only. Do not route the Ethernet cable outside of the building. Exposure of the cables to lightning could create a safety hazard and damage the product.

Connect the Gateway to Your Computer

Before installing the gateway:

- Check with your service provider to ensure broadband cable access is available in your area. To set up a wireless network, you will need a high-speed Internet connection provided by an Internet service provider.
- Choose a central location in your home where your computer and gateway are preferably near existing cable and electrical wall outlets.

***Note**: The following steps you through the wired Ethernet connection process so that you can quickly confirm that the gateway was properly connected and you can access the Internet.*

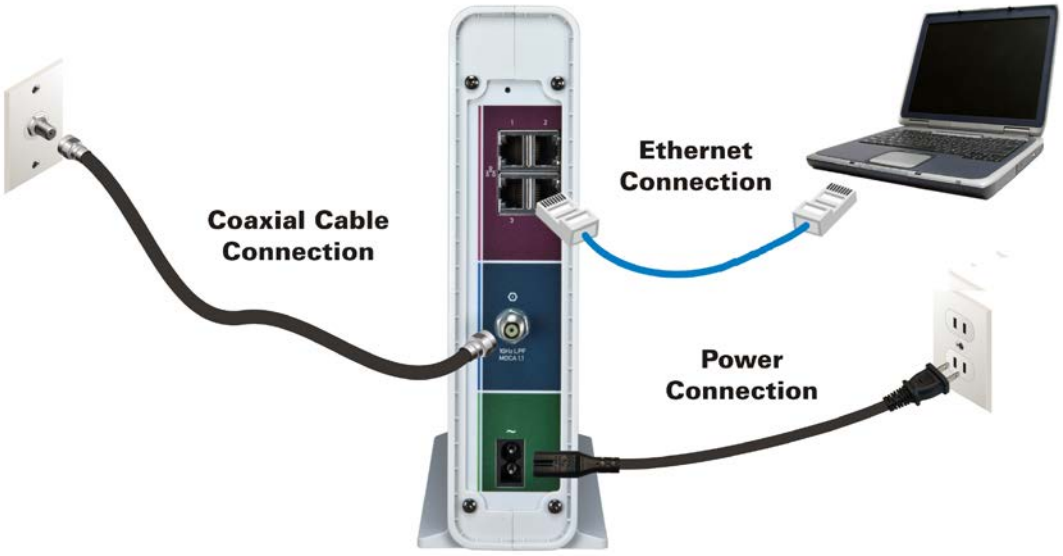


Figure 3 – SBG6782-AC Connection Diagram

1. Check that a coaxial cable is already connected to a cable wall outlet or RF splitter (optional).
2. Connect the other end of the coaxial cable to the Cable connector on the gateway. Use your hand to tighten the connectors, to avoid damaging them.

3. Connect the Ethernet cable to any available Ethernet port on your gateway and to the Ethernet port on your computer.

   Repeat for each additional computer or Ethernet–enabled device that you want connected on your wired network.

4. Connect the power cord to the Power port on the gateway and then plug it into an electrical wall outlet.

   ***Note**: This automatically powers ON your gateway.*

Test the Gateway Connections

Although your computer may already be configured to automatically access the Internet, you should still perform the following gateway connectivity test to verify that the devices were connected properly.

1. Power ON your computer and then log on.
2. Check that the **Power**, **Receive**, **Send**, and **Online** front panel LEDs on the gateway first FLASH in sequential order and then light SOLID. See Front Panel for additional LED status information.

   If an LED did not light SOLID, call the ARRIS SURFboard Technical Support Center at **1-877-466-8646** for assistance.

3. Contact your service provider to activate (provision) your gateway.

   ***Note**: Your service provider may allow for automatic activation which will automatically launch a special website when you open a web browser.*

4. Once your gateway is provisioned, open a web browser on your computer, such as Internet Explorer, Firefox, Google Chrome, or Safari.
5. Type a valid URL (for example, www.arrisi.com/consumer) in the address bar and then press **Enter**.

The ARRIS website should open. If it did not open, you may have to manually set up the network options on your computer to access the Internet. See Setting Up an Internet Connection for more information or call ARRIS SURFboard Technical Support (**1-877-466-8646**) for assistance.

Connect Your MoCA-Enabled Devices

You can also connect any MoCA-enabled devices such as the Motorola SBM1000 SMART Video Adapters or a Smart TV to the SBG6782-AC. You will need an RF cable splitter and an additional coaxial cable to connect the MoCA device and SBG6782-AC gateway. Follow the instructions included with the device to complete the applicable connections.

***Note**: The MoCA LED on the SBG6782-AC front panel will light SOLID green when the gateway detects other MoCA-enabled devices on your home network.*

4 Setting Up an Internet Connection

IMPORTANT! Your computer may already be configured to automatically access the Internet. If so, **do not** change the network options on your computer. Please contact ARRIS SURFboard Technical Support for assistance or verification.

If you cannot access the Internet after installing the gateway, you may have to manually set up your computer to connect to the Internet. To do this, you will have to enable the network options on your computer to automatically obtain an IP address and DNS server address. After configuring the network options, you should verify the IP address.

If you still cannot access the Internet after configuring the IP address, contact ARRIS SURFboard Technical Support for assistance.

Please note, operating system-specific commands for configuring computer network options are not provided in this document. The same general steps provided below apply to the following Microsoft Windows operating systems:

- Windows 8
- Windows 7
- Windows Vista
- Windows XP

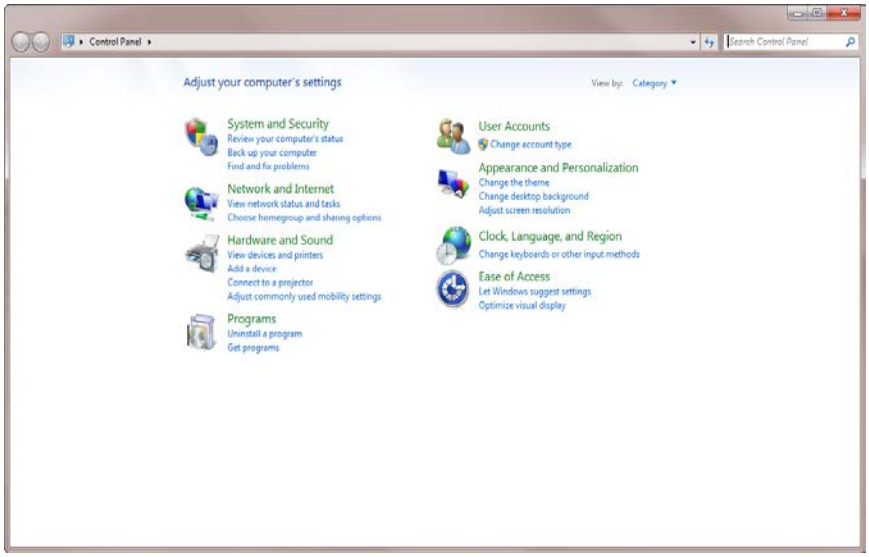
***Note**: For Mac, UNIX, and Linux computers, please follow the instructions provided in the applicable user documentation. Your service provider may provide additional instructions to help you set up your computer.*

If you are unfamiliar with the network configuration commands for your operating system or need assistance, we highly recommend that you contact your service provider or refer to the user documentation for the Windows operating system running on your computer for more information.

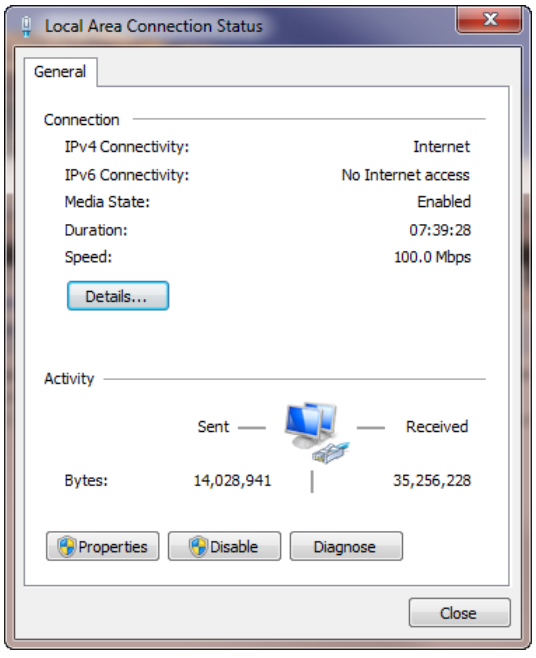
Configure Your IP Address

***Note**: The following instructions apply to Windows 7. Some windows and commands used in this procedure may differ slightly from your computer depending on your operating system.*

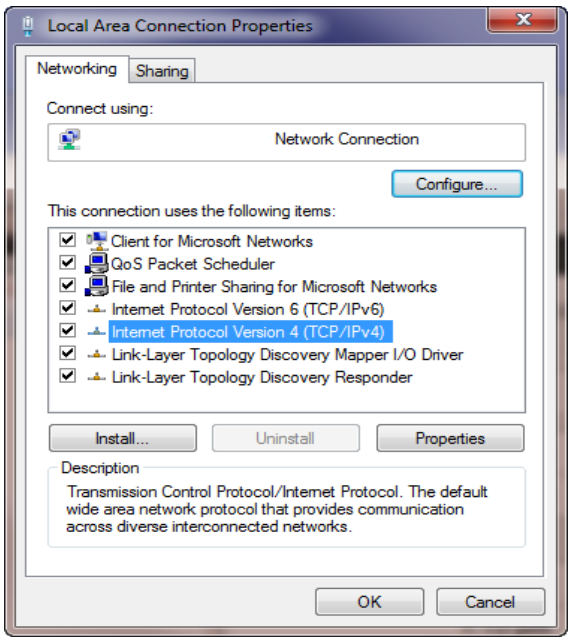
1. Open the **Control Panel** or **Network Connections** using the **Start** button from the taskbar on your computer desktop.
2. Click **View network status and tasks** to open the Network and Sharing window.



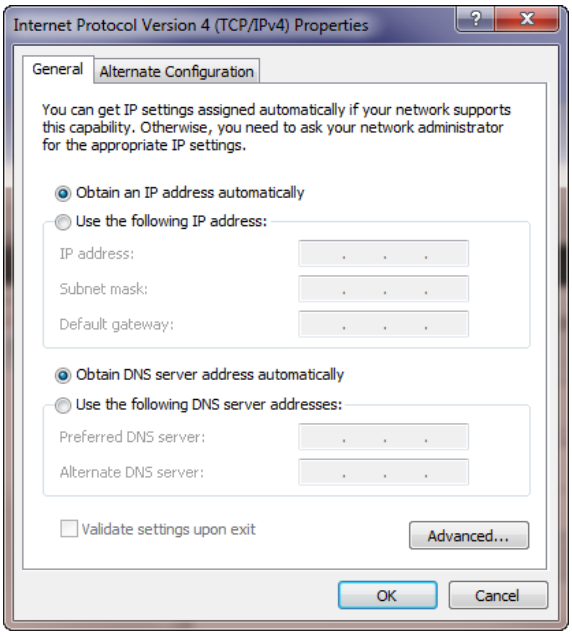
3. Click **Change adapter settings** from the Control Panel Home pane to open the Network Connections window.
4. Click **Local Area Connection** to open the Local Area Connection Status window.



5. Click **Properties** to open the Local Area Connection Properties window.



6. Select **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties** to open the TCP/IPv4 Properties window.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

7. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
8. Click **OK** to save the TCP/IP settings and close the Internet Protocol Properties window.
9. Step through to close the remaining windows and exit.

Verify & Renew Your IP Address

1. Open a command prompt window using the **Start** button and **Run** command from the Taskbar on your desktop.
2. Type **cmd** and click **OK** to open a command prompt window.
3. Type **ipconfig** and press **Enter** to display the IP configuration.
4. To renew the IP address, type **ipconfig/renew** and press **Enter**. A new IP address for your computer or other Ethernet-enabled device will display.
5. Type **exit** and then press **Enter** to return to Windows.

5 Setting Up a Wireless Network Connection

Your SBG6782-AC gateway and computer must have access to a Broadband or high-speed Internet service before setting up a wireless network connection. Also, make sure your computer and the SBG6782-AC are connected through an Ethernet connection.

Your SBG6782-AC gateway and computer must have access to a Broadband or high-speed Internet service before setting up a wireless network connection. Also, make sure your computer and the SBG6782-AC are connected through an Ethernet connection.

Choose one of the following options to set up your wireless network connection:

- Launch the Quick Start Wizard to Set Up Your Wireless Network
- Manually Set Up a Wireless Network on Your Computer
- Connect Your WPS-Enabled Devices

After setting up your wireless network connection, check that the wireless network connection was set up properly. See Test Your Wireless Network Connection for more information

Launch the Quick Start Wizard to Set Up Your Wireless Network

The SBG6782-AC Quick Start Wizard is a six-step application to help you quickly configure your basic wireless network settings. Depending on your home network setup, you can further customize your wireless home network configuration after completing the wizard.

1. Open any web browser on the computer connected to the SBG6782-AC.
2. In the Address bar, type **`http://192.168.0.1`** for the SBG6782-AC Web Manager IP address, and then press **Enter**. The gateway Login screen displays.
3. Type the default username and password. Both entries are case-sensitive.

   Username: **admin**

   Password: **motorola**

   ***Note**: The gateway login process may differ slightly depending on if you purchased the SBG6782-AC gateway from a retail store or if you received it from your service provider.*

4. Click **Login** to open the SBG6782-AC Web Manager. The Launch Quick Start Wizard screen displays (see Figure 4 on next page).
5. Click **Launch Quick Start Wizard** to start the wizard.
6. Click **Next**.

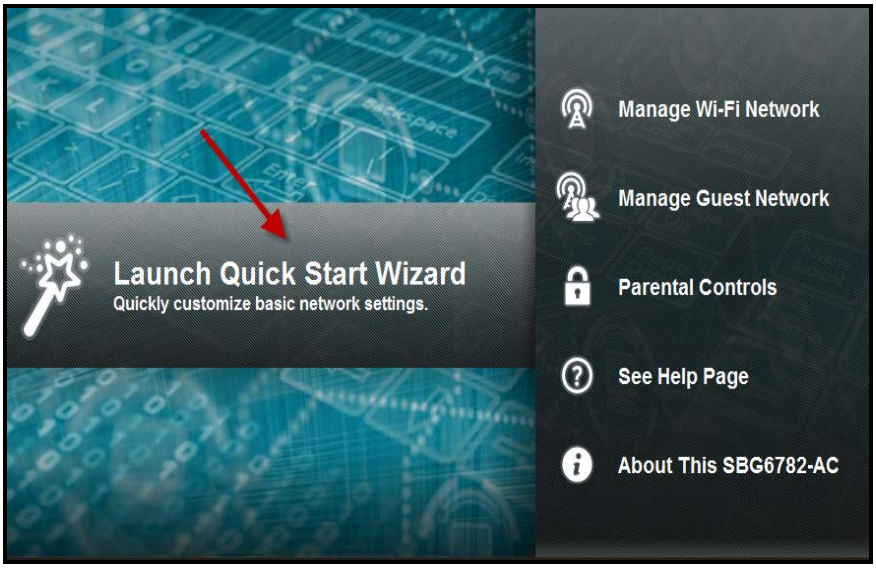


Figure 4 – SBG6782-AC Quick Start Wizard Screen

7. Enter a **Network Name (SSID)** for your wireless network.

   The network name must contain from one to 32 alphanumeric characters.
8. Enter a Passphrase or Wi-Fi Security Key and then click **Next**.

   This is the sign-on access code for your wireless network. The code must contain from 8 to 64 characters consisting of any combination of letters, numbers, and symbols.

   Remember that your passphrase should be as unique as possible to protect your wireless network and deter hackers or unauthorized access to your network.
9. **2.4 GHz** and **5 GHz** network configurations are created for your wireless network. Click **Next.**

   The Wi-Fi security type is created. The WPA2-PSK security code is the strongest security default.
10. Click **Next** to start the Wi-Fi Security mode.

    WPA2-PSK, the default security code, is automatically set and the network settings are displayed.
11. Click **Apply** to accept or **Previous** to change the configuration.

Manually Set Up a Wireless Network on Your Computer

***Note**: The steps for setting up a wireless network may differ slightly depending on the Windows operating system running on your computer. The following steps apply to Windows 7 systems.*

1. From the Windows taskbar, click **Start** button and then click **Control Panel**.
2. Click **View network status and tasks.**
3. Click **Set up a new connection or network**.
4. Click **Connect to the Internet**.

   ***Note**: The **You are already connected to the Internet** message may appear. Ignore this*

message and proceed with the next step.

5. Click **Set up a new connection anyway** and then click **Wireless**.
6. Scroll down and select the **MOTOROLA** wireless network name (see **SSID-2.4** listed on the SBG6782-AC gateway label located on the bottom of the gateway).

   Notes:

   - ***SSID-2.4*** *lists the default network name assigned to your wireless network.* ***2.4*** *refers to the 2.4 GHz Wi-Fi frequency range used by most wireless devices. The 5 GHz frequency provides better performance, if your device is capable of performing at that frequency level. However, the 2.4 GHz is more widely used and is compatible with a higher number of wireless devices.*
   - *We recommend that you use the default SSID name assigned to your gateway (located on the gateway label). You have the option to change the network name to one that may be easier for you to remember.*
7. Enter **Network security key code** in the Security key field (see **WPA-PSK** code listed on the SBG6782-AC gateway label) and then click **OK** to complete the wireless network connection.

   A Connected status message showing the wireless network connection should display.
8. Close the Wireless Network Connection window.

Connect Your WPS-Enabled Devices

Note*: Use the WPS Pairing button option to connect your wireless devices. Your computer hardware must support WPS and also have WPA security compatibility.*

1. Power ON the gateway and other WPS-enabled devices that you want to connect to a wireless network.
2. Press the **WPS** button located on the top of the SBG6782-AC.
3. Press and hold the **WPS** button on your WPS-enabled computer or other device for 5 to 10 seconds.
4. Repeat step 3 for each additional WPS-enabled device.

Test Your Wireless Network Connection

Perform the following test to verify that the SBG6782-AC and other wireless devices can connect to your wireless network:

1. If connected, disconnect the Ethernet cable from your computer and the SBG6782-AC.
2. Open a web browser on your computer.
3. Type a valid URL (for example, www.arrisi.com/consumer) in the address bar, and then click or press **Enter**.

   If the Motorola ARRIS website did not open, please call ARRIS SURFboard Technical Support at **1-877-466-8646** for assistance.

6 Managing Your Gateway and Connected Networks

Use the SBG6782-AC Web Manager to view and monitor the configuration settings and operational status of your gateway. You can also configure your network connections and wireless security settings.

Start the Gateway Web Manager

***Note**: Use the following default user name and password to log on to the SBG6782-AC Web Manager for the first time. For network security, we highly recommend that you change the user name and password after logging on. See Change the Default User Name and Password for more information.*

1. Open any web browser on the computer connected to the SBG6782-AC.
2. In the Address bar, type **`http://192.168.0.1`** for the SBG6782-AC Web Manager IP address, and then press **Enter**. The gateway Login screen displays.
3. Type the default username and password. Both entries are case-sensitive.

   Username: **admin**

   Password: **motorola**
4. Click **Login** to open the SBG6782-AC Web Manager. The Launch Quick Start Wizard screen displays

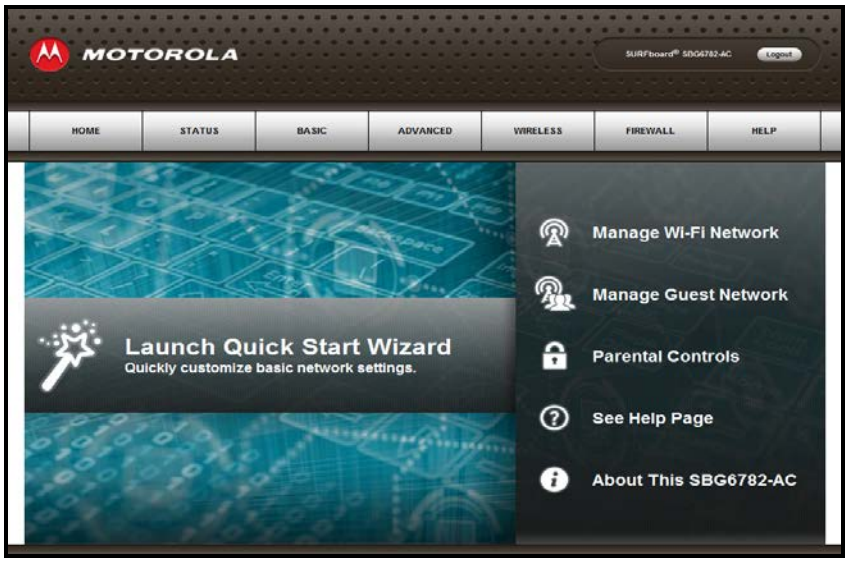


Figure 5 – Quick Start Wizard Opening Screen

***Note**: If you cannot access the HTML screens in the Gateway Web Manager, please call the ARRIS SURFboard Technical Support Center for assistance.*

Gateway Web Manager Menu Options

The SBG6782-AC main menu buttons are displayed along the top of the SBG6782-AC Web Manager screen. To display the drop-down submenu options, click the menu button.

Figure 6 – SBG6782-AC Web Manager Main Menu Buttons

The SBG6782-AC main menu and related submenu option links are also displayed along the bottom of the SBG6782-AC Web Manager screen. To open a submenu option, click the link.

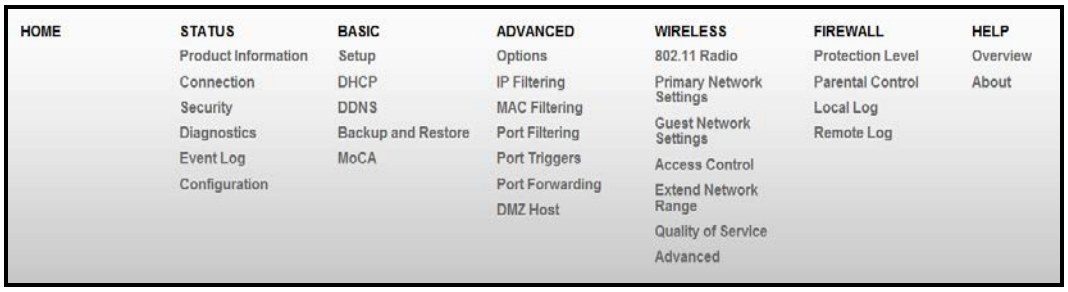


Figure 7 – SBG6782-AC Web Manager Main Menu Links

Table 4 – SBG6782-AC Web Manager Main Menu Options

MENU OPTION	FUNCTION
Home	Displays the Quick Start Wizard main screen
Status	Provides information about the gateway hardware and software, MAC address, gateway IP address, serial number, and related information. Additional screens provide diagnostic tools and also allow you to change your gateway user name and password.
Basic	Configures the gateway IP-related configuration data, including Network Configuration, WAN Connection Type, DHCP, and DDNS
Advanced	Controls Internet protocols which configure and monitor how the gateway routes IP traffic on the SBG6782-AC.
Wireless	Configures and monitors the gateway wireless networking features

MENU OPTION	FUNCTION
Firewall	Configures and monitors the gateway firewall
Help	Provides general information to help you set up your network
Logout	Closes the SBG6782-AC Web Manager

Get Help

You can choose any of the following three options to obtain help information for any SBG6782-AC Web Manager .function:

- General help information is available when you click **Help**, **Overview** on the SBG6782-AC Main Menu.

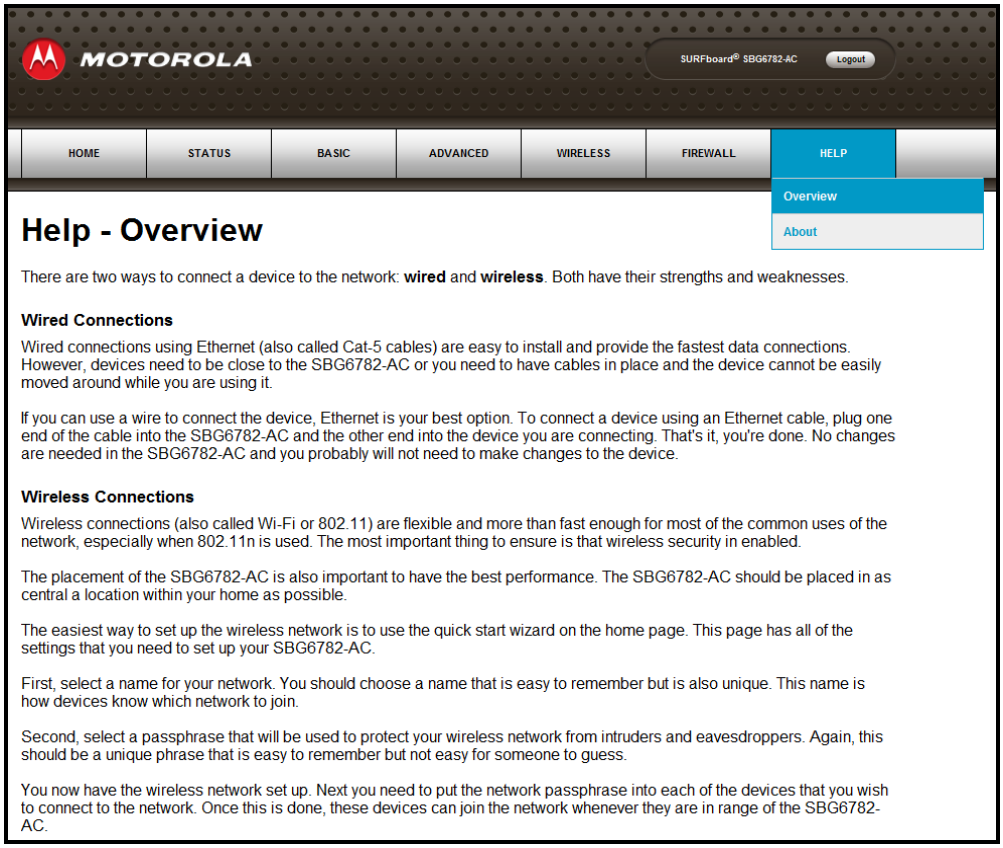

MOTOROLA
SURFboard® SBG6782-AC
Logout
HOME
STATUS
BASIC
ADVANCED
WIRELESS
FIREWALL
HELP
Overview
About
Help - Overview
There are two ways to connect a device to the network: wired and wireless. Both have their strengths and weaknesses.
Wired Connections
Wired connections using Ethernet (also called Cat-5 cables) are easy to install and provide the fastest data connections. However, devices need to be close to the SBG6782-AC or you need to have cables in place and the device cannot be easily moved around while you are using it.
If you can use a wire to connect the device, Ethernet is your best option. To connect a device using an Ethernet cable, plug one end of the cable into the SBG6782-AC and the other end into the device you are connecting. That's it, you're done. No changes are needed in the SBG6782-AC and you probably will not need to make changes to the device.
Wireless Connections
Wireless connections (also called Wi-Fi or 802.11) are flexible and more than fast enough for most of the common uses of the network, especially when 802.11n is used. The most important thing to ensure is that wireless security in enabled.
The placement of the SBG6782-AC is also important to have the best performance. The SBG6782-AC should be placed in as central a location within your home as possible.
The easiest way to set up the wireless network is to use the quick start wizard on the home page. This page has all of the settings that you need to set up your SBG6782-AC.
First, select a name for your network. You should choose a name that is easy to remember but is also unique. This name is how devices know which network to join.
Second, select a passphrase that will be used to protect your wireless network from intruders and eavesdroppers. Again, this should be a unique phrase that is easy to remember but not easy for someone to guess.
You now have the wireless network set up. Next you need to put the network passphrase into each of the devices that you wish to connect to the network. Once this is done, these devices can join the network whenever they are in range of the SBG6782-AC.

Figure 8 – Help Overview Screen

- Provides a concise list of your gateway configuration settings with applicable links for easy access when you click **Help**, **About** on the SBG6782-AC Main Menu. The link takes you to the related configuration screen.

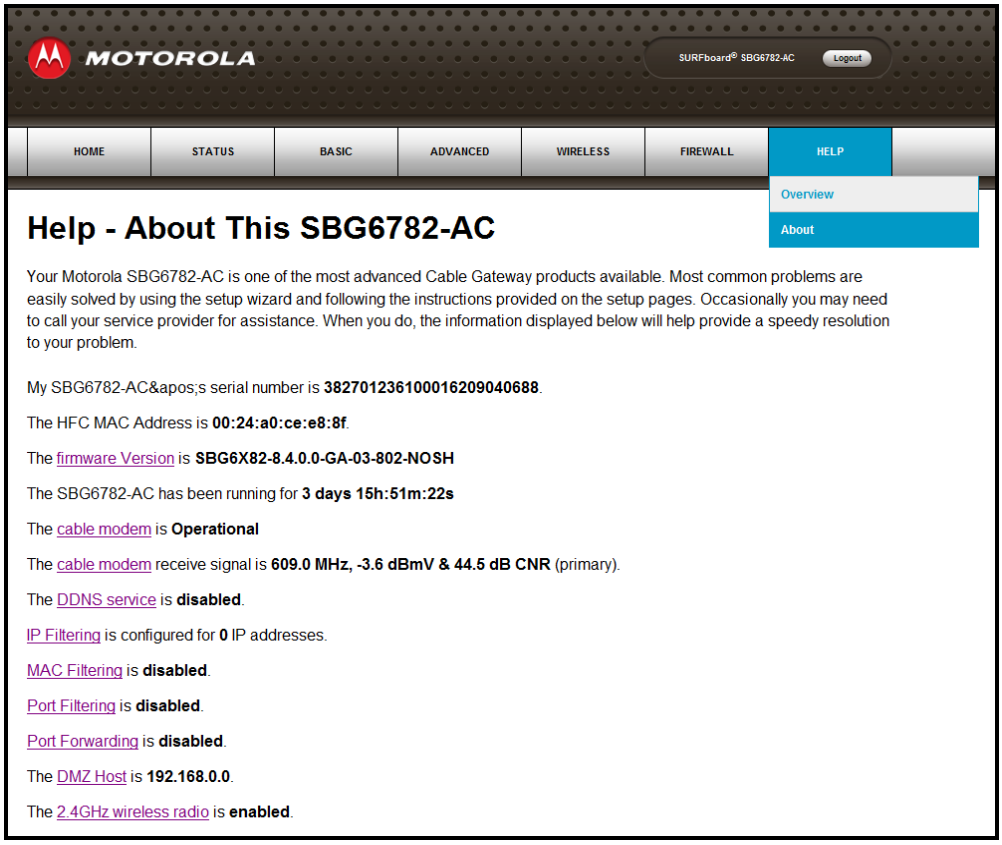

MOTOROLA
SURFboard® SBG6782-AC
Logout
HOME
STATUS
BASIC
ADVANCED
WIRELESS
FIREWALL
HELP
Overview
About
Help - About This SBG6782-AC
Your Motorola SBG6782-AC is one of the most advanced Cable Gateway products available. Most common problems are easily solved by using the setup wizard and following the instructions provided on the setup pages. Occasionally you may need to call your service provider for assistance. When you do, the information displayed below will help provide a speedy resolution to your problem.
My SBG6782-AC's serial number is 38270123610001620904068 8.
The HFC MAC Address is 00:24:a0:ce:e8:8f.
The firmware Version is SBG6X82-8.4.0.0-GA-03-802-NOSH
The SBG6782-AC has been running for 3 days 15h:51m:22s
The cable modem is Operational
The cable modem receive signal is 609.0 MHz, -3.6 dBmV & 44.5 dB CNR (primary).
The DDNS service is disabled.
IP Filtering is configured for 0 IP addresses.
MAC Filtering is disabled.
Port Filtering is disabled.
Port Forwarding is disabled.
The DMZ Host is 192.168.0.0.
The 2.4GHz wireless radio is enabled.

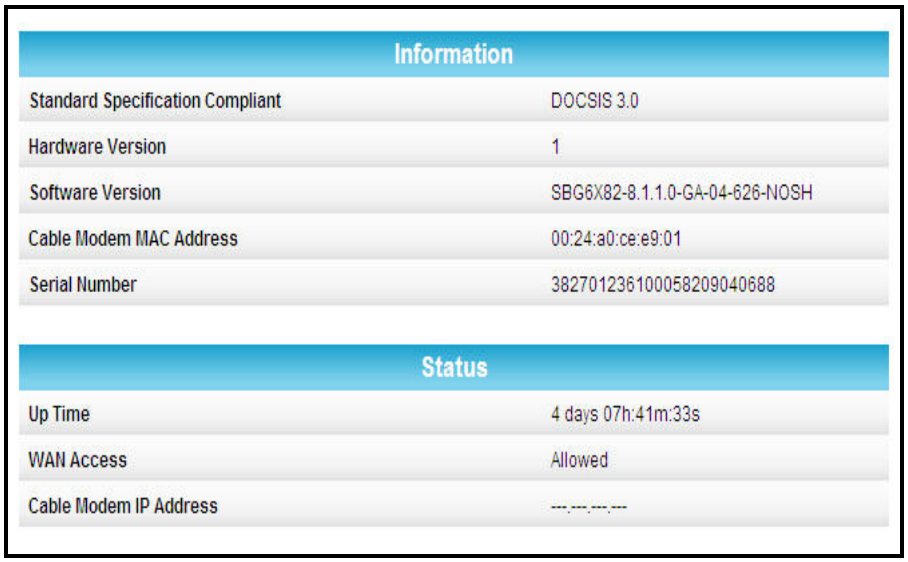
Figure 9 – Help About Screen

- More specific help information is available throughout the web manager for certain features when you click **Help** located to the right of the applicable field.

View the Gateway Product Information

The Status-Product Information screen displays general product information and the current operational status of the gateway.

1. Click **Status** on the SBG6782-AC Main Menu.
2. Click **Product Information** from the Status submenu options.
3. Click the **Refresh** button in your web browser to refresh the information on the screen.



Information	
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	1
Software Version	SBG6X82-8.1.1.0-GA-04-626-NOSH
Cable Modem MAC Address	00:24:a0:ce:e9:01
Serial Number	382701236100058209040688

Status	
Up Time	4 days 07h:41m:33s
WAN Access	Allowed
Cable Modem IP Address	---.---.---.---

Figure 10 – SBG6782-AC Status – Product Information Screen

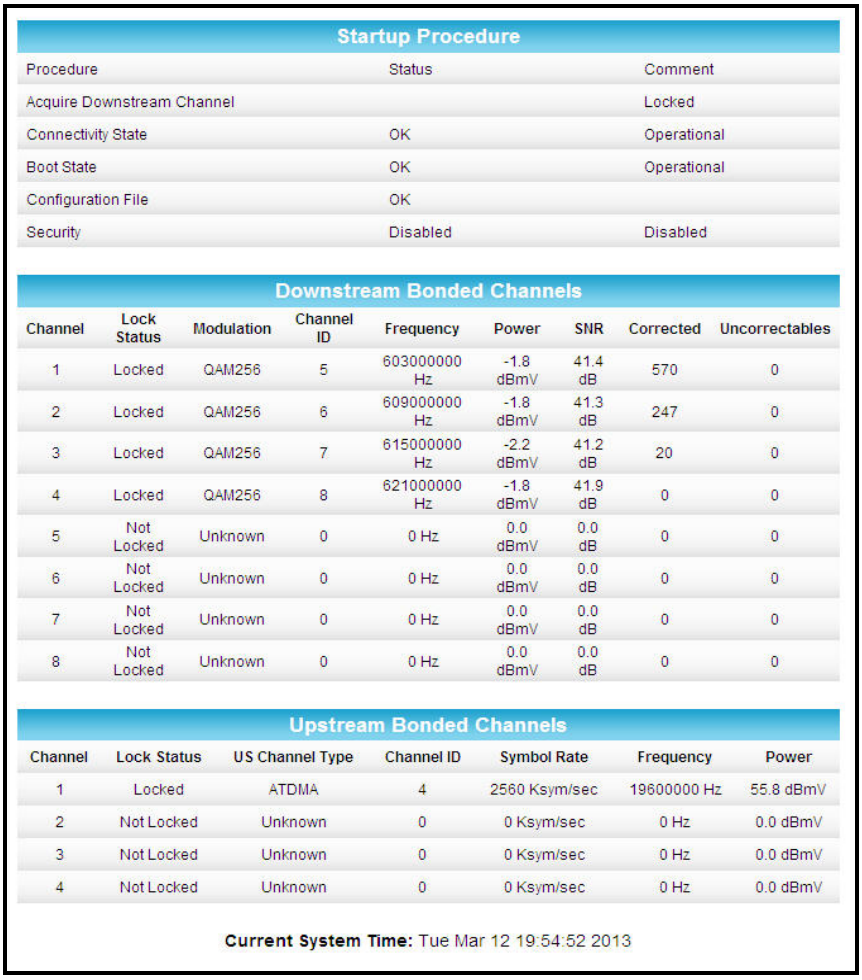
View the Gateway Status

The Status Connection screen displays information about the RF upstream and downstream channels, including downstream channel frequency, upstream channel ID, and upstream and downstream signal power and modulation.

This screen also displays IP lease information including the current IP address of the cable modem, the duration of both leases, the expiration time of both leases, and the current system time from the DOCSIS time server.

To open the Status Connection screen:

1. Click **Status** on the SBG6782-AC Main Menu.
2. Click **Connection** from the Status submenu options.



Startup Procedure

Procedure	Status	Comment
Acquire Downstream Channel		Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Configuration File	OK	
Security	Disabled	Disabled

Downstream Bonded Channels

Channel	Lock Status	Modulation	Channel ID	Frequency	Power	SNR	Corrected	Uncorrectables
1	Locked	QAM256	5	603000000 Hz	-1.8 dBmV	41.4 dB	570	0
2	Locked	QAM256	6	609000000 Hz	-1.8 dBmV	41.3 dB	247	0
3	Locked	QAM256	7	615000000 Hz	-2.2 dBmV	41.2 dB	20	0
4	Locked	QAM256	8	621000000 Hz	-1.8 dBmV	41.9 dB	0	0
5	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
6	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
7	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0
8	Not Locked	Unknown	0	0 Hz	0.0 dBmV	0.0 dB	0	0

Upstream Bonded Channels

Channel	Lock Status	US Channel Type	Channel ID	Symbol Rate	Frequency	Power
1	Locked	ATDMA	4	2560 Ksym/sec	19600000 Hz	55.8 dBmV
2	Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV
3	Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV
4	Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV

Current System Time: Tue Mar 12 19:54:52 2013

Figure 11 – SBG6782-AC Status Connection Screen

Back Up Your Gateway Settings

You can save a backup copy of the current gateway configuration settings to your local computer. You can use the backup file to restore your custom gateway settings in the event that you made changes that you no longer want.

To create a back up copy of your gateway settings:

1. Click **Basic** on the SBG6782-AC Main Menu.
2. Click **Backup and Restore** from the Basic submenu options.

Figure 12 – SBG6782-AC Backup and Restore Screen

3. Click **Choose File** and type the path and file name where you want to store the backup file on your computer, or search for an existing gateway configuration file that you want to update.
4. Click **Backup** to create a backup file of your SBG6782-AC configuration settings.

Restore Your Gateway Settings

WARNING! This action will delete your current gateway configuration settings and allow you to restore a previously saved gateway configuration.

***Note**: After the configuration settings are restored, the gateway will automatically reboot and you will have to log on using the default username (**admin**) and password (**motorola**).*

1. Click **Basic** on the SBG6782-AC Main Menu.
2. Click **Backup and Restore** from the Basic submenu options.
3. Click **Choose File** to search for a previously saved gateway configuration file.
4. Click **Restore**. The gateway will automatically reboot.

Reset to Factory Defaults

At any time, you can reset the SBG6782-AC gateway configuration and your user name and password back to the original factory settings.

WARNING! This process also deletes any custom gateway configurations you may have already created. We recommend that you create a backup copy of your gateway configuration before resetting the gateway. See Back Up Your Gateway Settings for more information.

From the SBG6782-AC Web Manager, do the following to open the Status Security screen:

1. Click **Status** on the SBG6782-AC Main Menu.
2. Click **Security** from the Status submenu options.

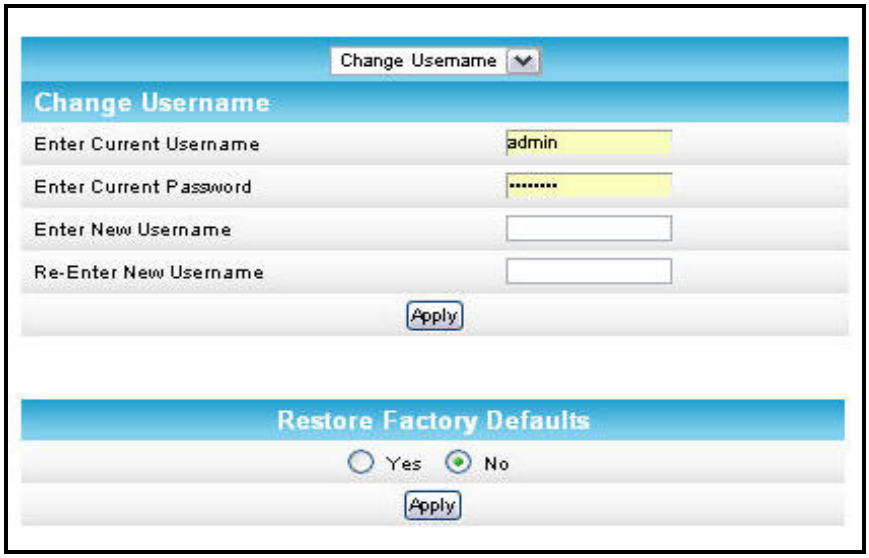


Figure 13 – Restore Factory Defaults

3. Select **Yes** under Restore Factory Defaults.
4. Click **Apply** to reset the default username and password, and restore the original gateway configuration.
5. Click **Logout** above the SBG6782-AC Main Menu bar in the upper right corner of the screen.
6. Log back in using the default username and password.

   Username: **admin**

   Password: **motorola**

Exit the SBG6782-AC Web Manager

To log out and close the SBG6782-AC Web Manager:

- Click **Logout** located in the upper right corner of the screen above the SBG6782-AC Main Menu.

7 Configuring Your MoCA Network

With the SBG6782-AC MoCA interface, you can create a reliable home network using your existing coaxial wiring. MoCA provides Internet Protocol (IP) connectivity with your set-top boxes, Smart TVs, and any other Ethernet-enabled electronic devices in your home. You can also use MoCA adapters to further extend your MoCA home network to connect additional Smart TVs, computers, gaming consoles, and other network devices.

You can enable or disable the SBG6782-AC MoCA interface. If the SBG6782-AC is not set up as the MoCA Network Controller, it will not have any control over the other devices on the MoCA network. If you disable the SBG6782-AC as the MoCA Network Controller, then you are allowing another device to become the MoCA Network Controller.

Set Up Your MoCA Network

1. From any screen, click the **Basic-MoCA** menu link or click the Basic menu button and then select **MoCA**.

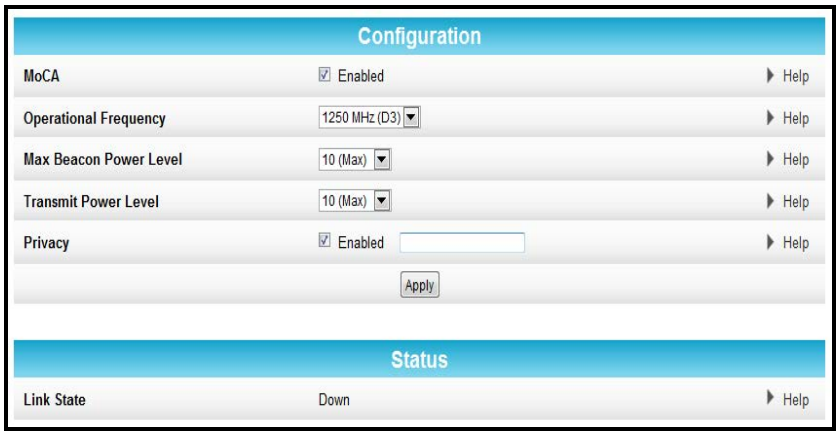


Figure 14 – MoCA Configuration and Status Screen

2. Select **Enabled** to set the SBG6782-AC as the MoCA Network Controller.
3. Select the operational frequency range for the MoCA data transmission rate from the list.
   - Normal range is between **1150 MHz to 1500 MHz**
   - Most cable TV systems use **1150 MHz**
4. Select the maximum number of beacon signals for data transmission. Default level is **10**.
5. Select the transmit Power level. Default level is **10**.
6. Select **Enabled** to require a 12 to 17 numeric digit password to allow the MoCA controller to encrypt data.

   ***Note**: The password must be the same on all devices on your home network.*
7. Click **Apply**.

8 Protecting & Monitoring Your Wireless Network

After you have successfully connected the SBG6782-AC gateway and your wireless devices, you should configure the gateway to protect your wireless network from unwanted and unauthorized access by any wireless devices within range of your wireless network. Although security for the SBG6782-AC gateway is already configured, you can use the SBG6782-AC configuration manager to tailor the level of security and access that you want to allow on your network.

Prevent Unauthorized Access

To prevent unauthorized access and configuration to your wireless network, we highly recommend that you immediately change the default user name and password after connecting to the Internet and logging on to the SBG6782-AC for the first time.

One of the most important recommendations for securing your wireless home network is to change the default administrator password on your SBG6782-AC and other wireless devices as well. Default passwords are commonly used and shared on the Internet.

To ensure that your wireless home network is secure, it is recommended that you follow these best practices for user passwords:

- Always create a secure password or pass phrase that is not easily guessed.
- Use phrases instead of names so that it may be easier for you to remember.
- Use a combination of upper and lowercase letters, numbers, and symbols.
- Continue to change your administrator password on a regular basis.

***Note**: If your service provider supplied the SBG7682-AC gateway, you may not have the necessary user privileges to change the log in user name.*

Change the Default User Name and Password

To change the default user name:

1. Log in to the SGB6782-AC from any web browser on your computer.
2. Type the Gateway Web Manager IP address, **`http://192.168.0.1`**, in the Address bar and then press **Enter**. The gateway Login screen displays.
3. Type the default username and password as they appear below.

   Username: **admin**

   Password: **motorola**
4. Click **Login** to open the SBG6782-AC Web Manager. The SBG6782-AC Status Connection screen displays.

5. Click the **Status** menu button and then click **Security** to display the Status Security screen.
6. Confirm that **Change Username** is displayed in the drop-down selection box.
7. Complete each field entry, but note the following:
   - o All fields (for example, Current Username & Current Password) are case-sensitive.
     ***Note**: For first-time logons:*
     - Current Username is **admin**
     - Current Password is **motorola**
   - o Make sure **No** is selected under **Restore Factory Defaults**

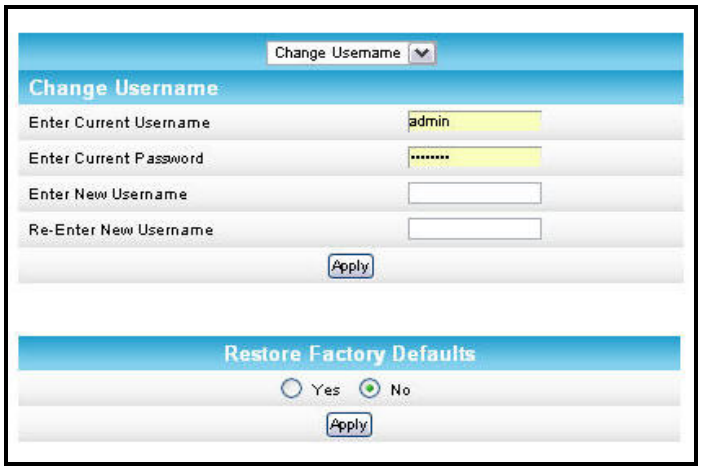


Figure 15 – Change Username

8. Click **Apply** to update your user name.
9. Click **Change Username** drop-down arrow to display **Change Password**.
10. Complete each field entry, but note the following:
    - o Username is the Current Username.
    - o All fields are case-sensitive.
    - o Make sure **No** is selected for **Restore Factory Defaults**.
    - o Find a secure place to write down and keep your new user name and password.
11. Click **Apply** to update your password.

Figure 16 – Change User Password

Set Up Firewall Protection

You can set up firewall filters and firewall alert notifications on your wireless home network. You can also block Java Applets, Cookies, ActiveX controls, popup windows, Proxies, and website access. See Protection Level for more information.

To set the firewall protection level:

1. From any screen, click the **Firewall-Protection Level** menu link or click the Firewall menu button on the SBG6782-AC Main Menu and then select **Protection Level**.

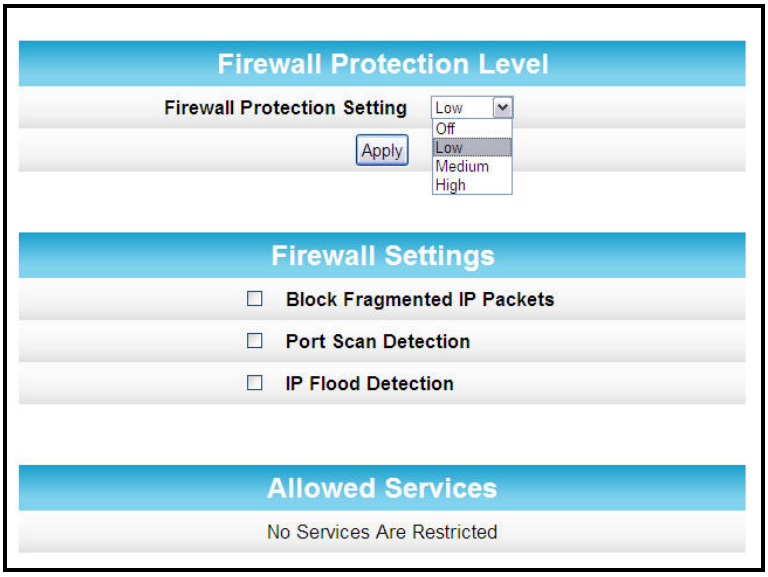


Figure 17 – Firewall Protection Level Screen

2. Click the Firewall Protection Setting drop-down button to select the firewall protection level. Possible values: **Low**, **Medium**, **High**, or **Off**

***Note**: Selecting **Off** will disable firewall protection on your home network. Your computer(s) and other Ethernet-enabled devices on your network will be at risk for possible attacks from viruses and hackers.*

3. Select each Web filter that you want to set for the firewall and then click **Apply**.

Set Up Parental Controls

You can set up the following Parental Controls on your home network:

- Allow or block access to specific Internet sites.
- Allow or block access to specific MAC addresses.
- Enable or disable Internet session duration timers to limit the amount of time for Internet access.

***Note**: Any Parental Control filters that do not include assigned ports, will apply to all ports. This also applies to MAC addresses as well.*

You can also link each user on your network to specified rules for login, time-access, and content filtering. See Parental Control for more information

To set Parental Controls:

1. From any screen, click the **Firewall-Parental Control** menu link or click the Firewall menu button on the SBG6782-AC Main Menu and then select **Parental Control**.
2. Click **Current Time Zone** drop-down button to select your time zone.

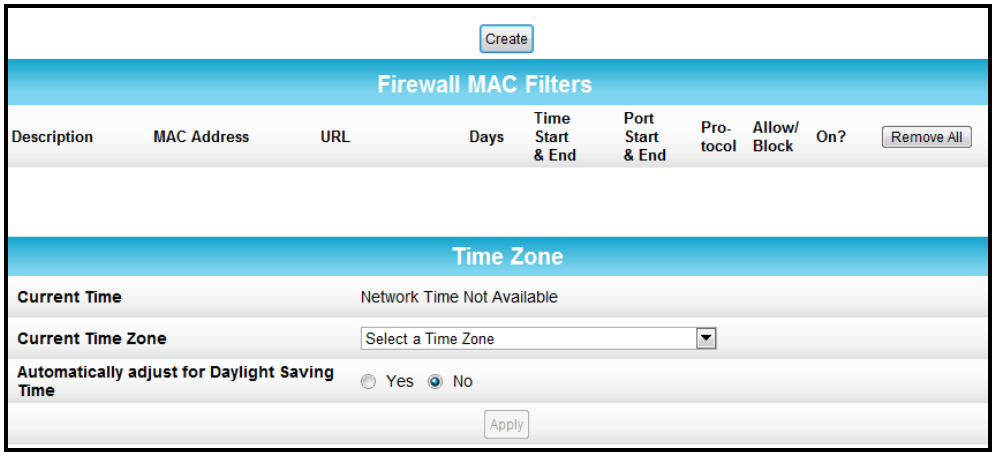


Figure 18 – Parental Control-Change Time Zone Screen

3. Select **Yes** or **No** to automatically adjust the time for Daylight Saving Time.
4. Click **Create** to continue setting up Parental Controls.

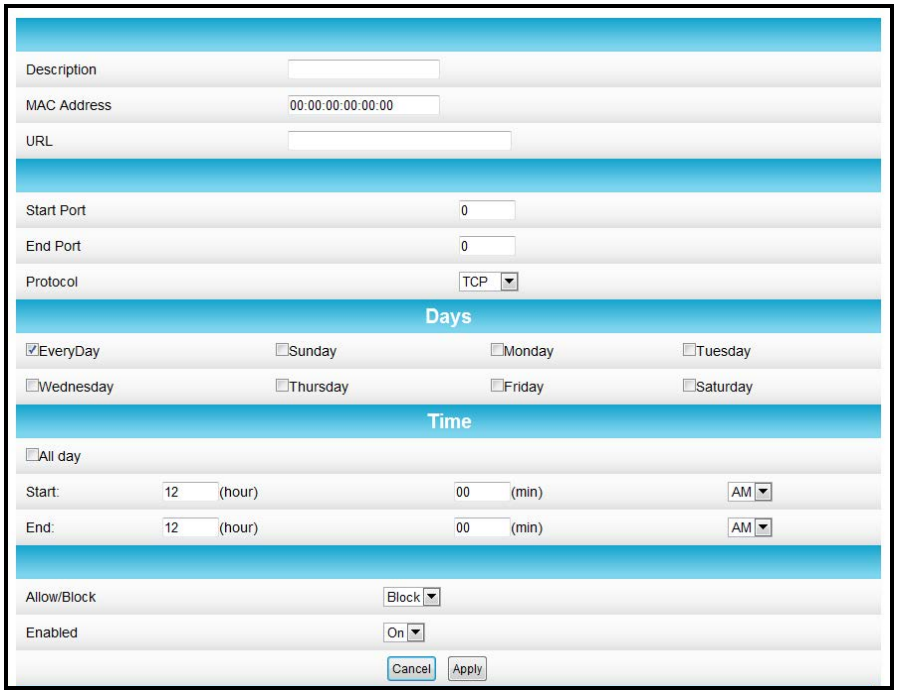


Figure 19 – Firewall Parental Control Screen

5. Enter a name for the user profile that you want to create in the Description field.
6. Enter the 12-digit (hexadecimal) MAC address of the device for which you are creating Parental Controls in the MAC Address field.
7. Enter the web address of the Internet site that you want to block or access.
8. Enter the Starting port number of the in the Start Port field.
9. Enter the Ending port number in the End Port field.
10. Select the days of the week that you want to allow the selected user to access the Internet.
11. Select the time range that you want to allow the selected user to access the Internet.
12. Select to **Allow** or **Block** Internet access for the time and days you set previously.
13. Select **On** or **Off** in the Enabled field to enable or disable this Parental Control restriction.
14. Click **Apply**, when done.

Set Up Port Triggers

You can use Port Triggers to configure dynamic triggers to specific devices on the LAN. This allows special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.

To configure Port Triggers:

1. From any screen, click the **Advanced-Port Triggers** menu link or click the Advanced menu button on the SBG6782-AC Main Menu and then select **Port Triggers**.
2. Click **Create Port Triggers** button to open the Add Port Triggering Entry window.

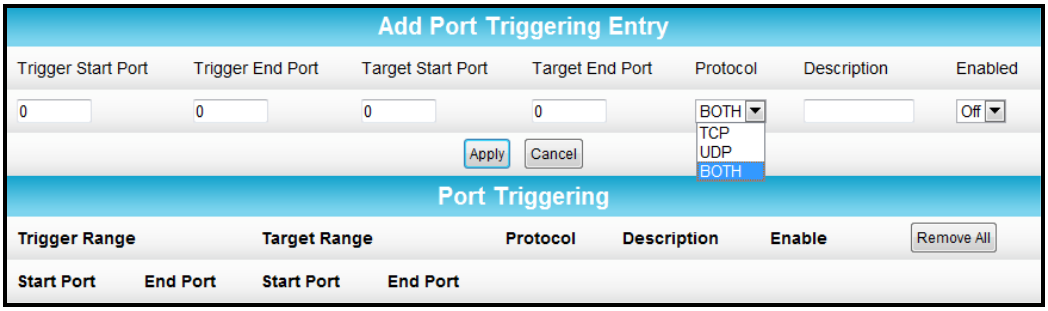


Figure 20 – Advanced Port Triggers Screen

3. Enter the starting port number of the Port Trigger range in the Trigger Start Port field.
4. Enter the ending port number of the Port Trigger range in the Trigger End Port field.
5. Enter the starting port number of the Port Trigger range in the Target Start Port field.
6. Enter the ending port number of the Port Trigger range in the Target End Port field.
7. Select **TCP**, **UDP**, or **Both** from the Protocol drop-down list.
8. Select **On** to activate IP port triggers or **Off** to disable IP port triggers.
9. Click **Apply** to create your port triggers.

Set Up the DMZ Host

WARNING! The gaming DMZ host is not protected by the SBG6782-AC gateway firewall. It is open to communication or hacking from any computer on the Internet. Consider carefully before configuring a device to be in the DMZ.

You can configure one computer to be the DMZ host. This setting is generally used for computers using problem applications that use random port numbers and do not function correctly with specific port triggers or the port forwarding setups. If you set up a computer as a DMZ Host, set this back to zero when you are finished with the needed application, since this computer will be effectively exposed to the public Internet, though still protected from Denial of Service (DoS) attacks via the Firewall.

To create the DMZ Host:

1. Click **Advanced** on the SBG6782-AC Main Menu.
2. Click **DMZ Host** from the Advanced submenu options.

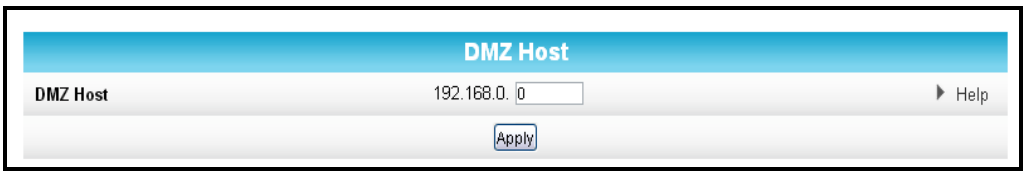


Figure 21 – Advanced DMZ Host Screen

3. Enter the last one to three digits (from **2** to **254**) of the IP address of the computer or gaming device you want to set up as the DMZ host and expose to the Internet.
4. Click **Apply** to activate the selected computer.

***Note**: Remember to set the IP address back to zero when you are finished with the needed application, since that computer will be exposed to the public Internet.*

Store Remote Firewall Logs

You can store firewall attack reports or logs on a computer in your home, so that multiple instances can be logged over a period of time. You can select individual attack or configuration items to send to the SysLog server, so that only the items of interest will be monitored.

***Note**: The SysLog server must be on the same network as the Private LAN behind the Configuration Manager (typically **192.168.0.x**).*

To store remote Firewall logs:

1. From any screen, click the **Firewall-Remote Log** menu link or click the Firewall menu button on the SBG6782-AC Main Menu and then select **Remote Log**.

Figure 22 – Firewall Remote Log Screen

2. Select all desired event types that you want to monitor. This will activate the SysLog monitoring feature.
3. Enter the last digits from **10** to **254** of the SysLog server's IP address.

   ***Note**: Normally, the IP address of this SysLog server is hard-coded so that the address always agrees with the entry on this page.*
4. Click **Apply**.

9 Troubleshooting Tips

If the solutions listed in this section do not resolve your problem, call the ARRIS SURFboard Technical Support Center at **1-877-466-8646** for assistance. You may be asked for the status of the LEDs as described in Front Panel LED Icons and Error Conditions.

You may have to reset the SBG6782-AC gateway configuration to its original factory settings if the gateway is not functioning properly.

Solutions

Table 5 – Troubleshooting Solutions

MODEM PROBLEM	POSSIBLE SOLUTION
Cannot access the Internet	Check the IP address. Follow the steps for verifying the IP address in Verify & Renew Your IP Address. If you need an IP address, call ARRIS SURFboard Technical Support for assistance.
POWER LED Icon is OFF	Check the power connection between the gateway and the electrical wall outlet. Check that the electrical outlet is working (is the outlet controlled by a light switch?). If so, disconnect and find another electrical wall outlet.
Cannot Send or Receive Data	Check each end of the coaxial cable connection on the gateway and cable outlet. Hand-tighten, if necessary. Check the Ethernet cable to make sure it is properly connected to the gateway and computer. On the front panel, check the status of the LED icons and refer to Front Panel LED Icons and Error Conditions to identify the problem. If you have cable television, check your television to ensure your cable service is operating properly.
Wireless devices cannot send or receive data	If the problem still persists after checking the coaxial cable and Ethernet connections and your IP address, check the **Security Mode** setting on the Wireless Primary Network screen. If you enabled **WPA** and configured a passphrase on the gateway, be sure each affected wireless client has the identical passphrase. If this does not solve the problem, check if the wireless client supports WPA. If you enabled **WEP** and configured a key on the gateway, be sure each affected wireless client has the identical WEP key. If this does not solve the problem, check whether the client's wireless adapter supports the type of WEP key configured on the gateway.

MODEM PROBLEM	POSSIBLE SOLUTION
Wireless devices cannot send or receive data (continued)	To temporarily eliminate the Security Mode as a potential issue, disable security. After resolving your problem, be sure to re-enable wireless security. On the Wireless Access Control Page, make sure the MAC address for each affected wireless client is correctly listed.

Front Panel LED Icons and Error Conditions

The SBG6782-AC front panel LED icons provide status information for the following error conditions:

Table 6 – Front Panel LED Icons and Error Conditions

LED ICON	STATUS	IF, DURING STARTUP:	IF, DURING NORMAL OPERATION
POWER	**OFF**	Modem is not properly plugged into the electrical outlet	Modem is unplugged
RECEIVE	**FLASHING**	Downstream receive channel cannot be acquired	Downstream channel is lost
SEND	**FLASHING**	Upstream send channel cannot be acquired	Upstream channel is lost
ONLINE	**FLASHING**	IP registration is unsuccessful	IP registration is lost
WIRELESS	**OFF**	LED is disabled	LED is disabled
WIRELESS	**OFF**	LED is disabled	LED is disabled
MoCA	**OFF**	No connected device is detected	Device is disconnected

A Gateway Configuration Screen Definitions

Basic Screens

The SBG6782-AC Basic screens allow you to view, monitor, and configure configuration data, including network configuration, LAN and WAN connection types, DHCP, and DDNS.

Setup

You can use the SBG6782-AC Basic Setup screen to view and configure the basic features of your SBG6782-AC gateway related to your service provider connection.

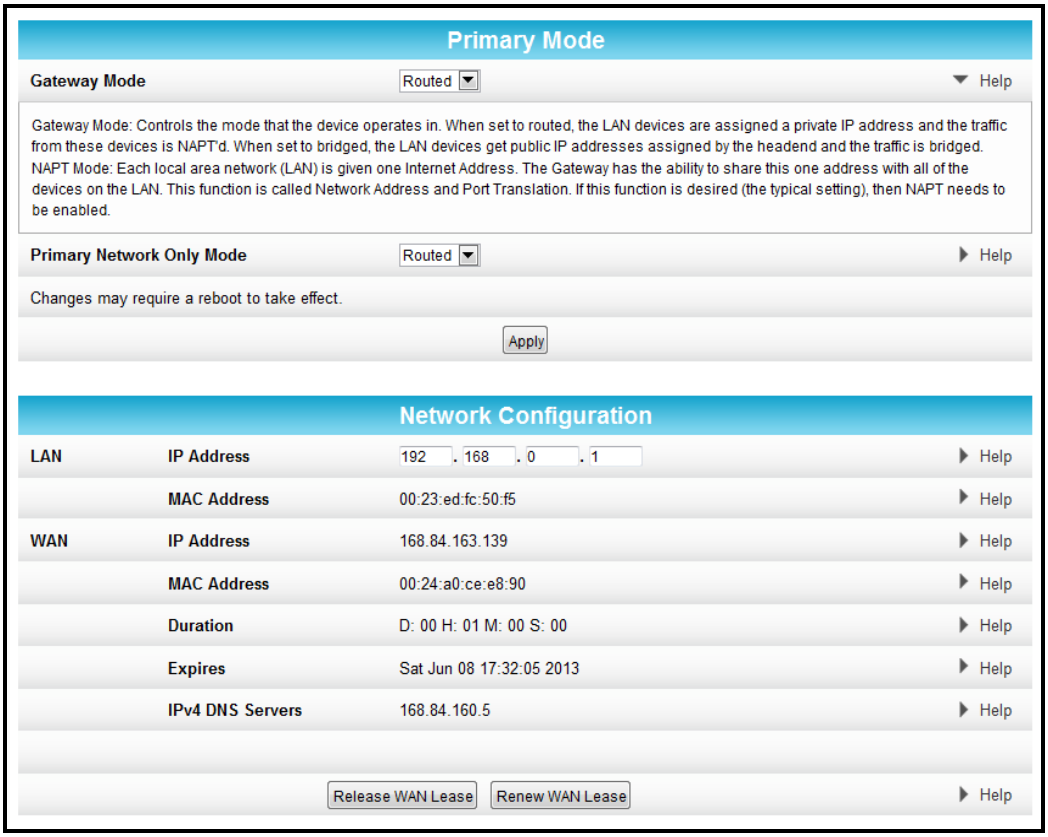

Primary Mode
Gateway Mode
Routed
Help
Gateway Mode: Controls the mode that the device operates in. When set to routed, the LAN devices are assigned a private IP address and the traffic from these devices is NAPT'd. When set to bridged, the LAN devices get public IP addresses assigned by the headend and the traffic is bridged. NAPT Mode: Each local area network (LAN) is given one Internet Address. The Gateway has the ability to share this one address with all of the devices on the LAN. This function is called Network Address and Port Translation. If this function is desired (the typical setting), then NAPT needs to be enabled.
Primary Network Only Mode
Routed
Help
Changes may require a reboot to take effect.
Apply
Network Configuration
LAN
IP Address
192 . 168 . 0 . 1
Help
MAC Address
00:23:ed:fc:50:f5
Help
WAN
IP Address
168.84.163.139
Help
MAC Address
00:24:a0:ce:e8:90
Help
Duration
D: 00 H: 01 M: 00 S: 00
Help
Expires
Sat Jun 08 17:32:05 2013
Help
IPv4 DNS Servers
168.84.160.5
Help
Release WAN Lease
Renew WAN Lease
Help

Figure 23 – Basic Setup Screen

Table 7 – Basic Setup Screen-Field Descriptions

FIELD	DESCRIPTION
Gateway Mode	Controls the device mode: **Routed**, **Bridged**, or **NAPT**
Primary Network Only Mode	Controls the primary network mode: **Routed**, **Bridged**, or **NAPT**
LAN	
IP Address	Enter the IP address of the SBG6782-AC on your private LAN.
MAC Address	Media Access Control address is set of 12 hexadecimal digits that are assigned during manufacturing to uniquely identify the hardware address of the SBG6782-AC access point.
WAN	
IP Address	The public WAN IP address of your SBG6782-AC, which is either dynamically or statically assigned
MAC Address	Media Access Control address — a set of 12 hexadecimal digits assigned during manufacturing that uniquely identifies the hardware address of the SBG6782-AC access point.
Duration	Describes how long before your Internet connection expires, The WAN lease will automatically renew itself when it expires.
Expires	Displays the exact time and date the WAN lease expires
Ipv4 DNS Servers	The addresses of the servers that convert web site names into Internet addresses assigned by the cable company.
Release WAN Lease	Click to release the WAN lease
Renew WAN Lease	Click to renew the WAN lease

DHCP

You can use the Basic DHCP (Dynamic Host Configuration Protocol) screen to configure the IP settings of your SBG6782-AC gateway and the DHCP server on your home network. You can also view the status of the optional internal SBG6782-AC DHCP server.

Do not modify these setting unless you are an experienced network administrator with a strong understanding of IP addressing, sub-netting, and DHCP.

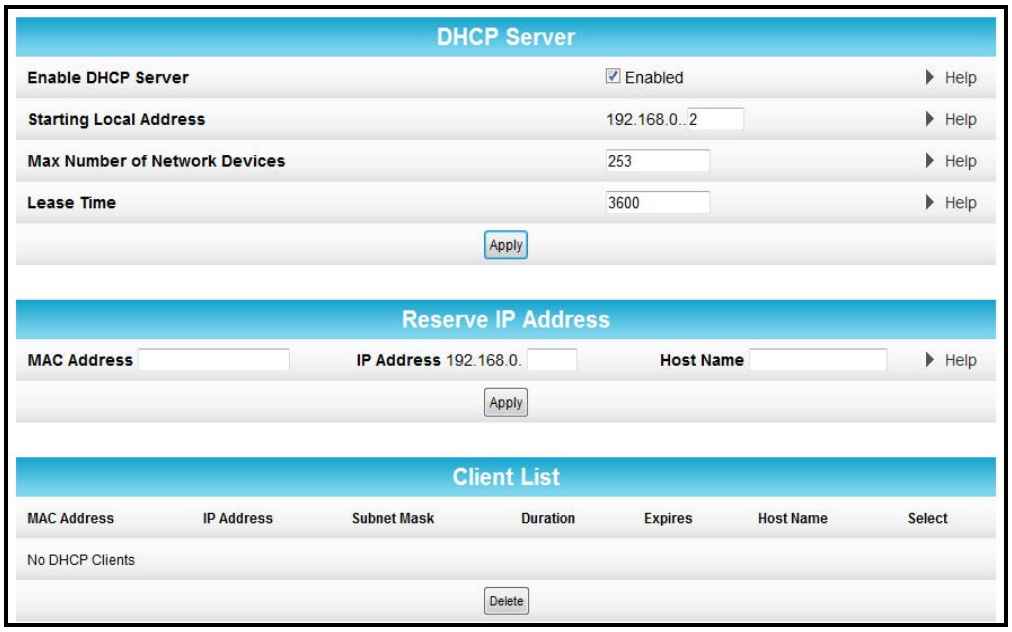


Figure 24 – Basic DHCP Screen

Table 8 – Basic DHCP Screen-Field Descriptions

FIELD	DESCRIPTION
Enable DHCP Server	Checkmark **Enabled** to enable the SBG6782-AC DHCP Server. Uncheck **Enabled** to disable the SBG6782-AC DHCP Server.
Starting Local Address	Enter the starting IP address to be assigned by the SBG6782-AC DHCP server to clients in dotted-decimal format. Default is **192.168.0.2**.
Max Number of Network Devices	Sets the maximum number of clients for the SBG6782-AC DHCP server to assign a private IP address.
Lease Time	Sets the time in seconds that the SBG6782-AC DHCP server leases an IP address to a client. The default is 3600 seconds (60 minutes).
Reserve IP Address	Lists the MAC address, IP address, and Host name of the DHCP client device.

DDNS

You can use the Basic DDNS (Dynamic Domain Name System) screen to set up the DDNS service to assign a static Internet domain name to a dynamic IP address. This allows various servers on the Internet to access your computer for processing your requests when you are visiting various Internet sites.

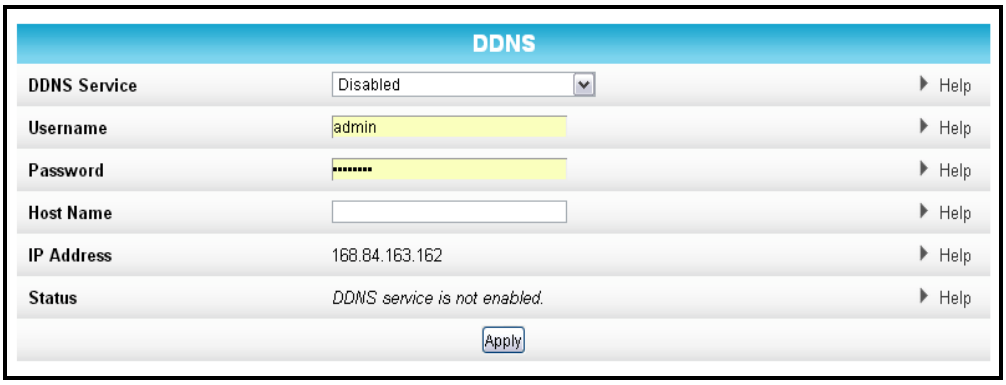


Figure 25 – Basic DDNS Screen

Table 9 – Basic DDNS Screen-Field Descriptions

FIELD	DESCRIPTION
DDNS Service	Select **Disabled** or select **wwwDynDNS.org** to enable the DDNS service
Username	Enter your DDNS user name
Password	Enter your DDNS Password
Host Name	Enter your DDNS Host Name
IP Address	Displays the IP address
Status	Shows if the DDNS service is **Enabled** or **Disabled**

Backup and Restore

You can use the Basic Backup and Restore screen to save a backup copy of the current SBG6782-AC gateway configuration settings locally on your computer or restore previously saved gateway configurations.

Figure 26 – Basic Backup & Restore Screen

Table 10 – Basic Backup & Restore-Field Descriptions

FIELD	DESCRIPTION
Restore	Restores a previously saved gateway configuration.
Backup	Creates a back up copy of the current gateway configuration.

MoCA

The MoCA Configuration and Status screen allows you to configure your MoCA home network.

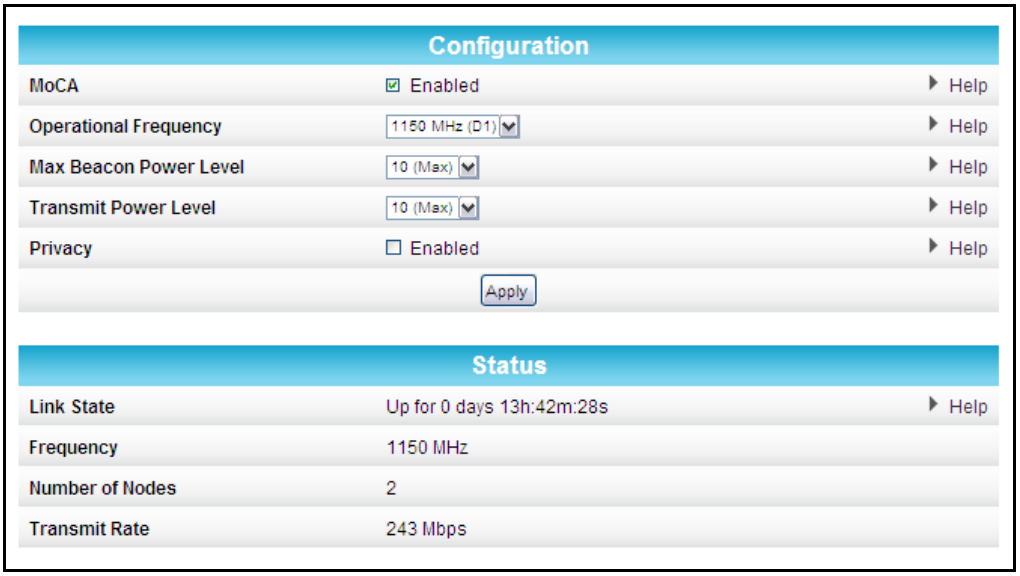


Figure 27 – Basic MoCA Configuration and Status Screen

Table 11 – Basic MoCA Screen-Field Descriptions

FIELD	DESCRIPTION
MoCA	Select **Enabled** or **Disabled** to turn ON or OFF your MoCA home network.
Operational Frequency	Frequency range for the MoCA data transmission rate. Normal range is from **1150 MHz** to **1500 MHz**
Max Beacon Power Level	Maximum number of beacon signals allowed for data transmission. Default is **10**.
Transmit Power Level	Power level for data transmission. Default is **10**.
Privacy	Turns ON or OFF data encryption. Create a **12** to **17** numeric digit password to allow the MoCA controller to encrypt data. Same password must be used on all devices on your home network.

Firewall Screens

You can configure firewall filters and alert notifications for your home network. The SBG6782-AC firewall protects the SBG6782-AC LAN from unwanted attacks and other intrusions on the Internet. Firewall protection also provides the following benefits:

- Advanced, integrated stateful-inspection firewall supporting intrusion detection, session tracking, and denial-of-service attack prevention.
- Maintains state data for every TCP/IP session on the OSI network and transport layers.
- Monitors all incoming and outgoing packets, applies the firewall policy to each one, and screens for improper packets and intrusion attempts.
- Generates comprehensive notifications for the following:
  - User authentications
  - Rejected internal and external connection requests
  - Session creation and termination
  - Outside attacks (intrusion detection)

Protection Level

The Firewall Protection Level screen has various settings related to blocking or exclusively allowing different types of data through the SBG6782-AC from the WAN to the LAN. There are three security firewall protection levels which correspond to how many services are allowed:

- **High** - Safest configuration, highest security
- **Medium** - Common configuration, modest risk
- **Low** - Minimum security, higher risk
- **Off** - No security, highest risk

Firewall protection enables the Stateful Packet Inspection (SPI) firewall features. Block Fragmented IP packets prevent all fragmented IP packets from passing through the firewall. Port Scan Detection detects and blocks port scan activity originating on both the LAN and WAN. IP Flood Detection detects and blocks packet floods originating on both the LAN and WAN.

You can block Java Applets, Cookies, ActiveX controls, pop up windows, and Proxies.

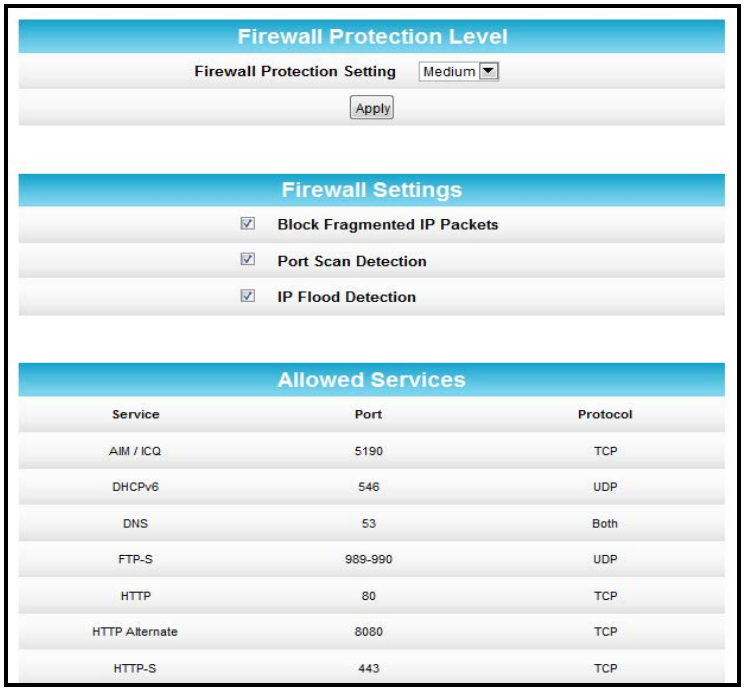


Figure 28 – Firewall Protection Level Screen

Table 12 – Firewall Protection Level Screen-Field Descriptions

FIELD	DESCRIPTION
Firewall Protection Level	Select **Low**, **Medium**, or **High** to set the level of firewall protection that you want for your gateway. Select **Off** to disable firewall protection. ***Note**: If you choose to disable firewall protection, your computer(s) and other Ethernet-enabled devices on your home network will be at risk for possible attacks from viruses and hackers.*
Firewall Settings	Checkmark to enable each filter that you want to set for the firewall. Click **Apply**, when done.
Allowed Services	Listing of the websites you selected to allow access to from your home network.

Parental Control

You can use the Parental Control screen to set up user access restrictions on a specific device connected to your SBG6782-AC network. You can set up the following Parental Controls:

- Allow or block access to specific Internet sites.
- Allow or block access to specific MAC addresses.
- Allow or block Internet access based on specific day and time settings.
- Enable or disable Internet session duration timers to limit the amount of time for Internet access.

***Note**: When creating Parental Control access filters, remember to assign the Start and End ports. Otherwise, any filters without assigned ports will apply to all ports. This also applies to MAC addresses.*

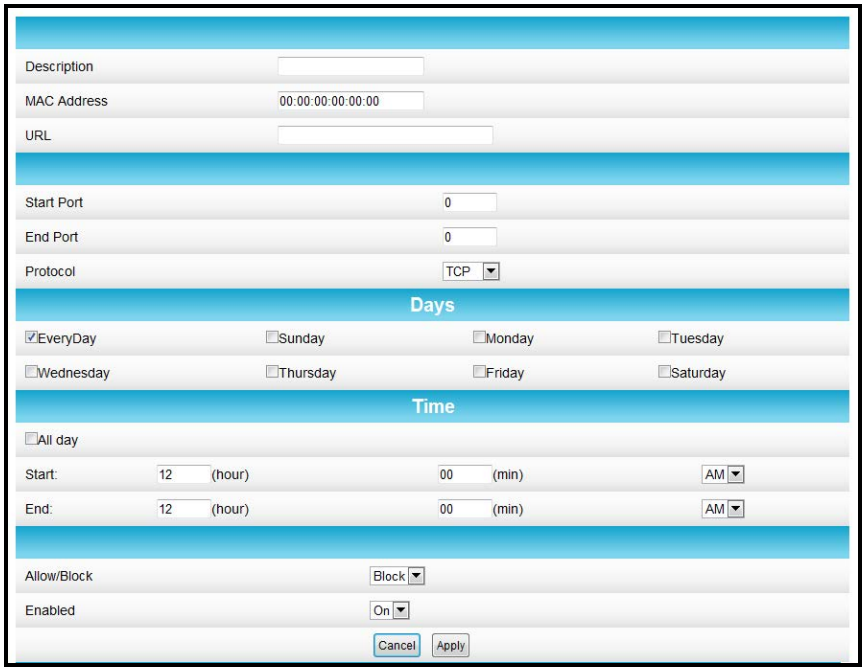


Figure 29 – Firewall Parental Control Screen

Table 13 – Firewall Parental Control-Field Descriptions

FIELD	DESCRIPTION
Description	Enter a name to create a new user profile.
MAC Address	Enter the 12-digit (hexadecimal) hardware address of the device that you are setting up for parental controls. The MAC addressed is assigned by the hardware manufacturer and should be located on the device label.

FIELD	DESCRIPTION
URL	Enter the web address of the Internet site that you want to block or access.
Start Port	Enter the starting port number of the range of ports for which you want to block incoming or outgoing access. Default port is **0**.
End Port	Enter the ending port number of the range of ports for which you want to block incoming or outgoing access. Default port is **0**.
Protocol	Select **TCP**, **UDP**, or **Both** for the Internet protocol.
Days	Select the days of the week that the selected user can access the Internet.
Time	Set the start and end time of day that the selected user can access the Internet.
Allow/Block	Set to allow or block Internet access for the time defined above.
Enabled	Turn ON or OFF this Parental Control restriction.

Local Log

You can send your firewall event log notifications in either of the following two formats:

- Individual e-mail alerts sent out automatically each time the firewall is under attack
- Local log stored within the gateway and displayed in table form on the Local Log page

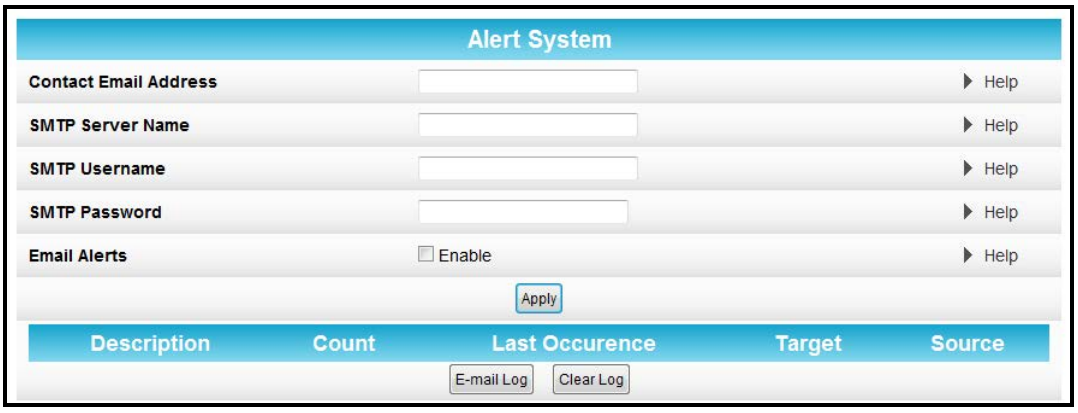


Figure 30 – Firewall Local Log Screen

Table 14 – Firewall Local Log Screen-Field Descriptions

FIELD	DESCRIPTION
Contact Email Address	Your email address.
SMTP Server Name	Name of the email Simple Mail Transfer Protocol (SMTP) server. Your email server name is required to send a firewall log to your email address. You can obtain the SMTP server name from your Internet service provider.
SMTP Username	User name for your email account. Check with your email provider.
SMTP Password	Password for your email account. Check with your email service provider.
Email Alerts	Enable or disable emailing firewall alerts.

Remote Log

You can send firewall attack reports out to a standard SysLog server, so that many instances can be logged over a long period of time. You can select individual attack or configuration items to send to the SysLog server so that only the items of interest will be monitored.

There are four types of Firewall reports that you can monitor and log:

- **Permitted Connections** – Select to notify the server to send you email logs identifying who is connecting to your network.
- **Blocked Connections** – Select to notify the server to send you email logs identifying who was blocked from connecting to your network.
- **Known Internet Attacks** – Select to notify the server to send you email logs of known Internet attacks against your network.
- **Product Configuration Events** – Select to notify the server to send you email logs of the basic product configuration events logs.

The SysLog server must be on the same network as the Private LAN behind the Configuration Manager (typically **192.168.0.x**).

To activate the SysLog monitoring feature, check all desired event types to monitor and enter the last byte of the IP address of the SysLog server. Normally, the IP address of this SysLog server is hard coded so that the address always agrees with the entry on this page.

Figure 31 – Firewall Remote Log Screen

Table 15 – Firewall Remote Log Screen-Field Descriptions

FIELD	DESCRIPTION
Permitted Connections	Select if you want email notification of who is connecting to your network.
Blocked Connections	Select if you want email notification of who is blocked from connecting to your network.
Known Internet Attacks	Select if you want email notification of known Internet attacks against your network.
Product Configuration Events	Select if you want email notification of the basic product configuration events.
to SysLog server at 192.168.0.x	Enter the last digit(s) of your SysLog server's IP address. Possible values: **10** to **254**

B Warranty Information

SURFboard SBG6782-AC DOCSIS 3.0 Wireless Cable Modem & Router
Motorola Mobility, LLC ("Motorola")

Retail Purchasers: If you purchased this Product directly from Motorola or from an authorized Motorola retail reseller, Motorola warrants to you, the original end user customer, that (A) the Product, excluding Software, will be free from defects in materials and workmanship under normal use, and (B) with respect to Software, (i) the media on which the Software is provided will be free from defects in material and workmanship under normal use, and (ii) the Software will perform substantially as described in its documentation. This Limited Warranty to you, the original end user customer, continues (A) for Software and the media upon which it is provided, for a period of ninety (90) days from the date of purchase from Motorola or an authorized Motorola reseller, and (B) for the Product (excluding Software), for a period of one (1) year from the date of purchase from Motorola or from an authorized Motorola reseller. To take advantage of this Limited Warranty or to obtain technical support, you must call the ARRIS/Motorola toll free phone number **1-877-466-8646**. Technical support charges may apply. Motorola's sole and exclusive obligation under this Limited Warranty for retail sales shall be to repair or replace any Product or Software that does not meet this Limited Warranty. All warranty claims must be made within the applicable Warranty Period.

Cable Operator or Service Provider Arrangements. If you **did not** purchase this Product directly from Motorola or from a Motorola authorized retail reseller, Motorola does not warrant this Product to you, the end-user. A limited warranty for this Product (including Software) may have been provided to your cable operator or Internet Service Provider ("Service Provider") from whom you obtained the Product. Please contact your Service Provider if you experience problems with this Product.

General Information. The warranties described in this Section shall not apply: (i) to any Product subjected to accident, misuse, neglect, alteration, Acts of God, improper handling, improper transport, improper storage, improper use or application, improper installation, improper testing or unauthorized repair; or (ii) to cosmetic problems or defects which result from normal wear and tear under ordinary use, and do not affect the performance or use of the Product. Motorola's warranties apply only to a Product that is manufactured by Motorola and identified by Motorola owned trademark, trade name or product identification logos affixed to the Product. Motorola does not warrant to you, the end user, or to anyone else that the Software will perform error free or without bugs.

MOTOROLA IS NOT RESPONSIBLE FOR, AND PROVIDES "AS IS" ANY SOFTWARE SUPPLIED BY 3RD PARTIES. EXCEPT AS EXPRESSLY STATED IN THIS SECTION ("WARRANTY INFORMATION"), THERE ARE NO WARRANTIES OF ANY KIND RELATING TO THE PRODUCT, EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR THE WARRANTY AGAINST INFRINGEMENT PROVIDED IN THE UNIFORM COMMERCIAL CODE. Some states do not allow for the exclusion of implied warranties, so the above exclusion may not apply to you.

What additional provisions should I be aware of? Because it is impossible for Motorola to know the purposes for which you acquired this Product or the uses to which you will put this Product, you assume full responsibility for the selection of the Product for its installation and use. While every reasonable effort has been made to insure that you will receive a Product that you can use and enjoy, Motorola does not warrant that the functions of the Product will meet your requirements or that the operation of the Product will be uninterrupted or error-free. MOTOROLA IS NOT RESPONSIBLE FOR PROBLEMS OR DAMAGE CAUSED BY THE INTERACTION OF THE PRODUCT WITH ANY OTHER SOFTWARE OR HARDWARE. ALL WARRANTIES ARE VOID IF THE PRODUCT IS OPENED, ALTERED, AND/OR DAMAGED.

THESE ARE YOUR SOLE AND EXCLUSIVE REMEDIES for any and all claims that you may have arising out of or in connection with this Product, whether made or suffered by you or another person and whether based in contract or tort.

IN NO EVENT SHALL MOTOROLA BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION OR ANY OTHER PECUNIARY LOSS), OR FROM ANY BREACH OF WARRANTY, EVEN IF MOTOROLA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO CASE SHALL MOTOROLA'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

These matters are governed by the laws of the Commonwealth of Pennsylvania, without regard to conflict of laws principles and excluding the provisions of the United Nations Convention on Contracts for the International Sale of Goods.

Retail Purchasers Only. If you purchased this Product **directly** from Motorola or from a Motorola authorized retail reseller, please call the ARRIS/Motorola toll-free number, **1-877-466-8646** for warranty service or technical support. Technical support charges may apply.

Cable Operator or Service Provider Arrangements. If you **did not** purchase this Product directly from Motorola or from a Motorola authorized retail reseller, please contact your Service Provider for technical support.

ARRIS Enterprises, Inc.
3871 Lakefield Drive, Suwanee, GA 30024

www.arrisi.com

365-095-23865 x.1 12/13